UNIVERSIDAD DE CÓRDOBA
FACULTAD DE FILOSOFÍA Y LETRAS
DPTO. DE TRADUCCIÓN E INTERPRETACIÓN, LENGUAS ROMANCES, ESTUDIOS SEMÍTICOS Y DOCUMENTACIÓN

Gestión terminológica y optimización del proceso de traducción especializada:

Aplicación en el ámbito de la seguridad informática

María José Pinilla Machado

2017

UNIVERSIDAD D CÓRDOBA

Dirigida por: María del Mar Rivas Carmona

TITULO: *GESTIÓN TERMINOLÓGICA Y OPTIMIZACIÓN DEL PROCESO DE TRADUCCIÓN ESPECIALIZADA: APLICACIÓN EN EL ÁMBITO DE LA SEGURIDAD INFORMÁTICA*

AUTOR: *María Josefa Pinilla Machado*

© Edita: UCOPress. 2017
Campus de Rabanales
Ctra. Nacional IV, Km. 396 A
14071 Córdoba

www.uco.es/publicaciones
publicaciones@uco.es

TÍTULO DE LA TESIS:

Gestión terminológica y optimización del proceso de traducción especializada: Aplicación en el ámbito de la seguridad informática

DOCTORANDO/A:

María Josefa Pinilla Machado - 30981738-W Programa de Lenguas y culturas

INFORME RAZONADO DEL/DE LOS DIRECTOR/ES DE LA TESIS
(se hará mención a la evolución y desarrollo de la tesis, así como a trabajos y publicaciones derivados de la misma).

La Tesis Doctoral *"Gestión terminológica y optimización del proceso de traducción especializada: Aplicación en el ámbito de la seguridad informática"* presentada por Dña. María Josefa Pinilla Machado es el fruto de un trabajo serio y tenaz de muchos años de investigación y práctica profesional.

La doctoranda es Traductora Jurada de Inglés y traductora *freelance* desde 2008. Ha realizado traducciones para diversas editoriales como Anaya Multimedia, entre las que destacan los trabajos sobre seguridad informática *Gestión de proyectos con Project 2007, Project 2010, iPad 2 a fondo* ó *Seguridad informática Comptia Segurity+.* En virtud de su experiencia y bagaje profesional, en diciembre de 2013 defendió bajo mi tutela el Trabajo Fin de Máster "Proyecto terminológico y traducción de textos del área de la seguridad informática: *Seguridad informática Comptia Segurity+. Guía de seguridad y certificación del examen SYO-301*" que mereció los más altos elogios. Ese brillante trabajo fue la semilla de la investigación que ahora presenta.

Esta tesis doctoral se centra en el análisis y la traducción de textos especializados en seguridad informática y, en concreto, incide en las ventajas que ofrece la implantación de herramientas terminológicas y de traducción asistida en la traducción especializada de textos de este ámbito. El corpus objeto de estudio está extraído del extenso manual *Comptia Segurity+* traducido por la autora de esta tesis en el año 2011.

En la actualidad la industria de la traducción proporciona servicios lingüísticos y tecnológicos que permiten a empresas y organismos de distinto tipo adaptar sus productos y servicios en un mundo globalizado. La seguridad informática se convierte en un requisito indispensable en estas situaciones comunicativas, dada la necesidad de proteger los sistemas de información de cualquier posible amenaza. Además, en un sector que evoluciona constantemente, la capacidad de actualización se vuelve imprescindible.

Dado el volumen de traducción generado, surge la necesidad paralela de implementar estrategias que optimicen el proceso de traducción especializada.

Una de estas herramientas para alcanzarlo es la realización de proyectos terminológicos como el que desarrolla la doctoranda. Este incluye un fichero terminológico bilingüe inglés>español de 165 fichas del ámbito de la seguridad informática, un glosario también bilingüe y un sistema jerarquizado de conceptos. Asimismo, el proyecto terminológico sirve de base para configurar un proyecto de traducción en Trados 2014 vinculado con Multiterm 2014, que culmina con la creación de una base de datos terminológica de indudables aplicaciones prácticas.

Dado que el número de glosarios, diccionarios o bases de datos sobre seguridad informática es realmente escaso, el recurso presentado cobra una especial relevancia. Su utilidad se comprende aún más si tenemos en cuenta que la seguridad informática está en continua expansión, por lo que esta base de datos, indudablemente, seguirá ampliándose y servirá de ayuda para profesionales de la informática, traductores, intérpretes o cualquier usuario de este tipo de textos.

En definitiva, se trata de un trabajo útil e innovador, de necesaria publicación. La autora ya ha presentado parte de los resultados de este trabajo en distintos foros como el XI Congreso Internacional Traducción, Textos e Interferencias (Baeza, julio 2014), el I Congreso Internacional Ciencia y Traducción (Córdoba, abril 2016) o el 1st International Summer School in Translation Technology (Amberes, septiembre 2016). Asimismo, ha publicado parte de sus resultados a través del artículo “Dificultades terminológicas en el proceso de traducción de un texto de seguridad informática” en la revista *Tonos Digital* (junio, 2016) o el capítulo “Cómo abordar la traducción de un encargo editorial desde un punto de vista holístico” en la editorial alemana Lit Verlag (2016).

Por último, quisiera expresar mi profunda satisfacción por la exitosa culminación de tan arduo y concienzudo trabajo de investigación.

Por todo ello, se autoriza la presentación de la tesis doctoral.

Córdoba, 23 de diciembre de 2016

Firma de la directora

Fdo.: Mª del Mar Rivas Carmona

Agradecimientos

A mis padres. Ellos han hecho posible que yo esté aquí hoy leyendo esta tesis doctoral. Gracias por haberme proporcionado una vida llena de amor y cuidados. Gracias por abrirme las puertas del estudio y el conocimiento.

A mi hermano, que siempre ha estado a mi lado de forma incondicional. Hermano, gracias por ser parte de mi vida. Quien tiene un hermano, tiene un tesoro. Seguiremos caminando, bro ;)

A mi tutora, María del Mar Rivas Carmona. Gracias por acompañarme y orientarme estos años. Sí, he aprendido muchas cosas teóricas sobre traducción, terminología e investigación. Pero también he mejorado como persona y eso sí que no tiene precio.

A todas las piedras que me he encontrado por el camino, que han sido algunas, por mantenerme alerta y despierta para seguir avanzando.

Contenido

1. INTRODUCCIÓN

El presente trabajo de investigación se centra en el análisis y la traducción de un tipo concreto de textos científico-técnicos, los textos especializados en seguridad informática. Este tipo de textos es un vivo ejemplo de cómo traducción y terminología son ámbitos de conocimiento que están estrechamente relacionados y cómo esta última puede cambiar por completo el proceso de traducción y la calidad del resultado final.

El corpus objeto de traducción y análisis que hemos seleccionado consiste en los cinco capítulos de mayor relevancia de un extenso manual de seguridad informática de referencia en su ámbito, que fue publicado por la editorial Anaya Multimedia y traducido por la autora de esta tesis en el año 2011. El proceso de traducción se llevó a cabo durante el período transcurrido desde el 10 de junio hasta el 7 de agosto de dicho año. El título del manual es *Seguridad informática CompTIA Segurity* +, y los capítulos elegidos por su especial interés son los que enumeramos a continuación:

- **Capítulo 2:** "Infraestructura y conectividad"
- **Capítulo 3:** "Proteger redes"
- **Capítulo 5:** "Control de acceso y gestión de identidad"
- **Capítulo 10:** "Seguridad física y basada en hardware (Mantrap)"
- **Capítulo 12:** "Seguridad de red inalámbrica"

Al tratarse de un tema especializado, cabe destacar que la persona encargada de realizar este encargo ya contaba con experiencia como traductora profesional y también había traducido textos de este campo de especialidad antes de trabajar con este manual. Por mencionar algunos títulos, podemos destacar las siguientes publicaciones traducidas por quien suscribe: *Gestión de proyectos con Project 2007*[1], *Project 2010*[2] o *iPad 2 a fondo*[3], publicados los dos en la Editorial Anaya Multimedia. Además, en la actualidad, seguimos en activo en la práctica profesional, traduciendo manuales de diversas temáticas. Esta trayectoria profesional ofrece un bagaje que permite analizar los diversos factores que influyen en el proceso de traducción, por

[1] E. J. MARMEL: *Gestión de proyectos con Project 2007*. Madrid: Anaya Multimedia, 2009.
[2] C. CHATFIELD Y T. JOHNSON: *Project 2010 (Paso A Paso)*. Madrid: Anaya Multimedia, 2011.
[3] D. HUISMAN: *iPad 2 a fondo*. Madrid: Anaya Multimedia, 2011.

ejemplo, las ventajas a todos los niveles que ofrece la implantación de herramientas terminológicas y de traducción asistida.

Sin lugar a dudas, justificar el porqué de la elección de este manual es de especial interés para este trabajo de investigación. ¿Qué nos hizo decantarnos por este título?, ¿qué tipo de selección realizamos?, ¿cuáles fueron los elementos de selección?... Aunque trataremos esta cuestión con mayor profundidad más adelante, podemos adelantar que una de las principales razones que nos hizo decantarnos por este título fue su naturaleza híbrida, es decir, el hecho de que se trata de un manual que no pertenece a una única tipología textual. Por un lado, como se puede observar a primera vista, se trata de un manual técnico sobre seguridad informática; no obstante, a su vez tiene una función didáctica añadida, puesto que pretende formar a técnicos informáticos para la preparación de un examen. De ahí, por ejemplo, que al final de cada capítulo encontremos tres apartados con fines claramente educativos: “Ideas clave para el examen”, “Prueba de evaluación” y “Respuestas de la prueba de evaluación”.

Las traducciones técnicas dominan el mercado. Esta afirmación tiene cada día más fuerza. Manuales, guías de instrucciones, fichas técnicas, documentación de productos, catálogos, listas de especie, peritajes, informes técnicos… En un mundo globalizado por completo, empresas, organismos gubernamentales u organizaciones sin ánimo de lucro se ven obligados a adaptar sus productos y servicios para sus clientes nacionales e internacionales. De hecho, se trata de algo esencial para su éxito y supervivencia. La industria de la traducción es la que proporciona servicios lingüísticos y tecnológicos que ayudan a implementar estas adaptaciones. Este fue otro factor determinante para la elección del tema.

Si concretamos un poco más, y de modo totalmente relevante para nuestra investigación, la seguridad informática es un requisito indispensable para todas las empresas, organismos gubernamentales u organizaciones sin ánimo de lucro. Proteger los sistemas de información, desde el más potente de los servidores hasta el más pequeño portátil, es esencial para los expertos y profesionales. Un profundo estudio de los sistemas, las redes, los programas y hasta del propio hardware es indispensable para prevenir amenazas futuras y eliminar las ya existentes. Se trata, además, de un sector que cambia y avanza de forma constante, por lo que las actualizaciones deben ser continuas.

La guía de estudio objeto de esta investigación es un referente a la hora de hacer frente al mundo inseguro que nos rodea. No solo aporta los conocimientos y habilidades necesarios para disponer de una formación profunda en materia de seguridad, sino que es, ante todo, un recurso para solucionar los retos profesionales. Este manual da las claves para acceder a la certificación SY0-301[4], de indudable prestigio profesional en materia de seguridad, y permite a sus lectores aprender todo lo necesario para poder aprobar el examen CompTIA[5], que otorgará al técnico un valor añadido en el mundo laboral. Las competencias profesionales de estos textos en materia de seguridad son también útiles y atractivas para quienes solo pretenden aprender o ponerse al día. El manual incluye, además, un CD-ROM con exámenes y ejemplos completos, así como provechosas herramientas y utilidades provenientes del libro original en inglés.

Como podemos observar, se trata de un texto dirigido a profesionales del sector. En consecuencia, el grado de especialidad es muy elevado y hemos de esperar un grado equivalente de alta densidad terminológica.

1.1 Motivos para la elección del tema

Tras barajar distintas temáticas especializadas y opciones textuales sobre las que llevar a cabo el presente trabajo de investigación, nos decantamos por este manual de seguridad informática por varios motivos. Entre ellos podemos destacar los siguientes:

* Las traducciones técnicas dominan el mercado.
* El texto en cuestión tiene naturaleza híbrida: técnico y didáctico.
* Son textos de alta densidad terminológica.
* La longitud del texto (650 páginas) permite extraer términos relevantes de un corpus real muy extenso sobre seguridad informática.

[4] Versión de examen de certificación CompTIA vigente hasta diciembre de 2014. La versión actual es SY0-401. Como cualquier certificación técnica, se actualiza con regularidad para estar al día de las tecnologías actuales.

[5] Siendo la mayor asociación de la industria mundial de las TIC, CompTIA desarrolla certificaciones que no están asociadas con ningún proveedor específico y que miden las destrezas de las TIC desde un nivel básico a experto.

- Se trata de un tema de actualidad en constante cambio y evolución.
- El texto sigue siendo un manual de referencia en su ámbito, puesto que no existen ediciones posteriores.
- El texto está publicado por editoriales de prestigio en las versiones origen y meta.
- Existe la posibilidad de futuras actualizaciones del manual, lo que permite el ***uso práctico de la base de datos terminológica y la memoria de traducción***.
- Hay un amplio mercado de publicaciones sobre seguridad informática e informática en general. Por lo tanto, una base de datos terminológica sobre este tema se puede utilizar en otros proyectos del mismo tema.

Nos gustaría detenernos en este punto, de forma breve, en los pormenores del encargo real que ha inspirado este trabajo, que serán detallados en el capítulo 4 "Encargo, hoja de proyecto, traducción y figuras".

Una agencia de traducción realizó el encargo del presente manual de informática de 650 páginas en 2011 a un traductor autónomo. La seleccionada fue la autora de este trabajo. El proyecto se llevó a cabo desde el 10 de junio hasta el 7 de agosto de 2011. Las unidades de entrega semanales eran 81 y estas incluían las figuras que aparecían en el texto.

La empresa, la editorial Anaya Multimedia, remitió un manual de estilo y formato con el propósito de que el resultado fuera homogéneo con el resto de títulos publicados. Sin embargo, las decisiones en torno a las estrategias de traducción, a las fases de investigación terminológica y al uso de herramientas de traducción recaen exclusivamente sobre una persona, en este caso, la traductora. En otras ocasiones, se establecen equipos de traducción en los que es aún más importante sentar las bases del proyecto desde el inicio para sistematizar el trabajo.

Como podemos observar, a pesar de la importancia del proyecto dada su temática y envergadura, la agencia de traducción no establece en ningún momento dentro de la programación y planificación del trabajo mención alguna a la fase de investigación terminológica. No obstante, al tratarse de un manual de formación, se llevó a cabo una revisión técnica para que los términos fueran adecuados y coherentes. Esto revela la importancia de la terminología en este

trabajo. Así pues, con la presente investigación ***nos proponemos dar prioridad a la fase terminológica y establecerla desde la fase más inicial del proyecto para simplificar la fase de revisión y sistematizar el programa de trabajo***.

El traductor también es el encargado de instalar todo el software necesario para realizar las capturas de pantalla en el idioma del texto meta. Este aspecto es muy importante, ya que la terminología especializada que aparece en el texto debe ser coherente con la que aparece en las capturas de pantalla para no crear confusión en el lector. Por lo tanto, hemos de tenerlo en cuenta a la hora de crear la base de datos terminológica para no ofrecer distintas traducciones de un mismo término en el texto meta, lo que sería deseable en otro tipo de textos como los humanístico-literarios, por ejemplo, pero no en el caso de un texto técnico de estas características en el que se requiere precisión absoluta.

Las agencias de traducción suelen gestionar de forma simultánea muchos proyectos para diversos clientes. Como cabe esperar, ellas dan prioridad a la rentabilidad, por lo que es poco probable que financien la fase terminológica de los proyectos. En estos casos, es el traductor el encargado de gestionar la terminología del proyecto.

1.2 Estructura del trabajo de investigación

El presente trabajo de investigación se ha estructurado de tal modo que se pudiera facilitar al máximo su lectura y comprensión. En todo momento hemos pretendido seguir un esquema lógico y progresivo, de lo general a lo particular, que permitiera llevar a cabo un análisis ordenado y llegar a los consiguientes resultados y conclusiones relevantes.

- **Introducción:** El objetivo de este epígrafe es explicar brevemente el encargo, comentar el perfil profesional de la autora del encargo y de esta tesis, destacar la doble revisión de la que es objeto la traducción del manual y mencionar las rutas profesionales a las que se dirige.
- **Contextualización lingüística:** El objetivo de este apartado es describir el tipo de texto objeto de investigación, especialmente sus

características lingüísticas. Procediendo desde lo general a lo específico, se repasarán los rasgos propios de los textos especializados en general; a continuación se revisarán las características propias de los textos técnicos y los textos didácticos; nos detendremos en los rasgos de los manuales técnicos y, finalmente, estudiaremos los manuales de seguridad informática, en particular.

- **Fundamentos teóricos y metodología:** En este capítulo nos centraremos en la disciplina de la Terminología aplicada a la traducción, dado que es el enfoque prioritario en nuestro análisis y dada la importancia que cobra en este manual. Por otra parte, también se argumentará acerca de la gran utilidad de los ficheros y glosarios terminológicos, así como de los sistemas de conceptos. Todo ello sienta las bases de este trabajo de investigación y da mayor sentido al pequeño proyecto terminológico realizado a partir de los dos capítulos seleccionados para el análisis.

  Además, en este apartado se explicará la metodología seguida durante la realización de este proyecto, deteniéndonos en las etapas del mismo, definiendo en detalle el porqué de la elección del tema, las tutorías y el trabajo que se realizó en ellas, etc.

- **Encargo, hoja de proyecto, traducción y figuras:** Este capítulo contiene información relacionada con la elaboración del proyecto de traducción. Se indican las fechas, los plazos, las unidades por entrega, el tipo de revisiones que se llevaron a cabo, el formato de las figuras y las capturas de pantalla, y demás factores que determinaron el encargo de traducción.

- **Memoria de traducción:** Previo al análisis terminológico se detalla la memoria de traducción en la que se recogen las dificultades terminológicas, el modo de solventarlas, así como otro tipo de problemas que han surgido a lo largo del proceso de traducción. La lectura de este epígrafe resulta altamente relevante para entender la necesidad de un análisis terminológico, que es la esencia de este trabajo. La aplicación práctica de la memoria de traducción y el proyecto terminológico será la creación de un proyecto de traducción en Trados 2014 y una base de datos terminológica que parta de los resultados obtenidos en Multiterm 2014.

- **Proyecto terminológico:** La realización de este proyecto constituye uno de los objetivos esenciales del presente trabajo de investigación, dados los fundamentos teóricos y toda la información analizada con anterioridad. Aquí se incluye un fichero terminológico que contiene 165 fichas de términos que aparecen en los dos capítulos analizados, un glosario bilingüe y un sistema de conceptos que agrupa los términos seleccionados. Este proyecto terminológico será el punto de partida para configurar el proyecto de traducción en Trados 2014 vinculado con Multiterm 2014. Nuestro proyecto terminológico se convierte en una base de datos terminológica mediante el volcado de datos a un documento de Excel y, de ahí, a Multiterm. De este modo, llegamos al día a día del traductor especializado para demostrar la necesidad de un análisis terminológico y sus aplicaciones prácticas.

- **Resultados:** Este apartado resume con brevedad los resultados obtenidos gracias a la realización del análisis y proyecto terminológico. También analizamos los resultados alcanzados con la creación de una base de datos terminológica en Multiterm 2014 integrada en Trados 2014.

- **Conclusiones:** Este epígrafe reúne las conclusiones fundamentales a las que se ha llegado gracias a la elaboración del presente trabajo de investigación.

- **Bibliografía:** Por último, se encontrarán las fuentes utilizadas para la realización de este trabajo ordenadas por libros, capítulos o artículos, diccionarios, bases de datos y páginas Web.

- **Apéndices:**

    - **Texto meta:** Este apartado del trabajo de investigación contiene la traducción del texto original. En este caso, se trata de cinco capítulos del libro *Seguridad informática CompTIA Segurity* +, en concreto los siguientes:

        - **Capítulo 2:** Infraestructura y conectividad
        - **Capítulo 3:** Proteger redes
        - **Capítulo 5:** Control de acceso y gestión de identidad
        - **Capítulo 10:** Seguridad física y basada en hardware (Mantrap)
        - **Capítulo 12:** Seguridad de red inalámbrica

* **Texto original:** Este apartado del trabajo de investigación contiene los cinco capítulos correspondientes del texto original. En este caso, se trata de los siguientes capítulos del libro *CompTIA® Segurity +™. Study Guide*:

  - ***Chapter 2:*** *Infrastructure and Connectivity*
  - ***Chapter 3:*** *Protecting Networks*
  - ***Chapter 5:*** *Access Control and Identity Management*
  - ***Chapter 10:*** *Physical and Hardware-Based Security*
  - ***Chapter 12:*** *Wireless Networking Security*

1.3 Objetivos

El presente trabajo de investigación parte de una serie de premisas y objetivos que detallaremos a continuación. Esto no solo permite optimizar tiempo y recursos, sino que, además, nos lleva a la realización de una investigación más exhaustiva y pormenorizada de los aspectos en los que queremos centrarnos desde el inicio. No obstante, no se trata de un listado rígido y cerrado, ya que, como investigadores, sabemos que durante el transcurso del trabajo pueden surgir nuevos temas y objetivos de interés que incluiremos y tendremos en cuenta para futuras líneas de investigación.

En el epígrafe de conclusiones y resultados se detallarán los objetivos que se han ido incorporando a nuestros propósitos iniciales y cuáles hemos destinado a futuras líneas de investigación.

Los objetivos se establecieron en un principio en base a la propia experiencia, dado el perfil profesional como traductora de manuales técnicos de inglés a español. Así, en una investigación que une terminología y traducción desde el principio, nos propusimos como primer objetivo:

1. ***Profundizar en las posibilidades que ofrecen tanto la terminología como las herramientas terminológicas en la traducción de manuales técnicos.***

No obstante, también quisimos dar un enfoque práctico y funcional a nuestra investigación. Queríamos llevar a cabo una investigación que plasmara los resultados obtenidos con una herramienta de uso real para los traductores profesionales y para los estudiantes de terminología. Por tanto, desde la fase inicial, nuestro segundo propósito ha sido:

2. ***Elaborar una herramienta terminológica útil y flexible, susceptible de ser modificada en el futuro para recoger la evolución del manual objeto de estudio o de otros posibles proyectos.***

Lenguaje y tecnología son algo vivo, que evoluciona con el paso del tiempo. Por ello, el resultado práctico de esta investigación es una herramienta creada a partir de los objetivos iniciales, pero abierta a evolución y adaptaciones en función del desarrollo de la tecnología y el lenguaje.

A estos objetivos principales se unen unos objetivos secundarios que detallamos a continuación. Se puede observar que priman los terminológicos, ya que para la realización de nuestro análisis textual requeríamos de unas características muy concretas en el corpus, especialmente, la densidad terminológica. Sin embargo, no perdemos de vista el enfoque práctico y real. El objetivo de la investigación siempre debe aportar mejoras para profesionales, estudiantes e investigadores. Los objetivos secundarios son:

- Analizar la densidad terminológica de un texto especializado del ámbito científico-técnico, en concreto del ámbito de la seguridad informática.
- Analizar las necesidades y objetivos del proyecto de traducción.
- Analizar las posibilidades de la gestión terminológica para la traducción.
- Analizar el encargo de traducción como proceso holístico en que intervienen diversos actores (traductor o equipo de traductores, maquetador, agencia de traducción, etc.).
- Aplicar herramientas de gestión terminológica a un proyecto real.
- Analizar en detalle qué tipo de información hay que gestionar: categoría de datos.
- Demostrar el carácter holístico de los proyectos de traducción en los que confluyen diversos ámbitos del saber.

- Demostrar las innumerables ventajas de unir terminología y traducción en la práctica profesional del traductor.
- Demostrar que la fase de investigación terminológica es especialmente importante para establecer la terminología específica del texto meta. (Sobre todo para proyectos grandes en los que intervienen varios traductores.)
- Demostrar que los traductores profesionales deben conocer las bases teóricas de la terminología.
- Demostrar que los traductores profesionales deben conocer y utilizar herramientas de gestión terminológica en su práctica profesional, ya que les lleva a mejores resultados y mayor calidad.
- Describir algunas de las herramientas de gestión terminológica más actuales que ofrece el mercado.
- Describir las características fundamentales de un texto didáctico.
- Describir las características fundamentales de un texto híbrido.
- Describir las características fundamentales de un texto técnico.
- Destacar el uso de software informático y memorias de traducción para agilizar el proceso de traducción.
- Destacar la estrecha relación entre terminología y traducción.
- Destacar la importancia de la búsqueda documental para la traducción de textos especializados.
- Destacar la importancia de la gestión de la terminología especializada.
- Destacar la importancia de un análisis terminológico para la traducción.
- Enfatizar la importancia de la fase de investigación terminológica para abordar proyectos de traducción.
- Establecer unos parámetros básicos para seleccionar los términos que pasarán a formar parte de la base de datos terminológica.
- Implementación de herramientas de gestión terminológicas en proyectos de traducción y enfatizar la mejora que suponen.

- Incorporar nuevas tecnologías al proceso de traducción.
- Profundizar en la búsqueda documental.
- Realizar un volcado terminológico en una base de datos terminológica para su posterior uso en futuros proyectos.
- Realizar un volcado terminológico en una memoria de traducción para su posterior uso en futuros proyectos.
- Seleccionar y desarrollar un software de traducción asistida adecuado.

Como podemos observar, objetivos teóricos y prácticos se entrelazan para dotar a esta investigación con un enfoque teórico-práctico. Una vez desarrollados los objetivos teóricos de forma exhaustiva, los aplicaremos con el fin de implementar estas mejoras a la práctica profesional del traductor en aras de una mayor calidad y profesionalidad.

Definir los objetivos desde el punto de partida de este trabajo de investigación nos ha permitido acotar nuestro análisis y localizar con mayor agilidad los puntos clave para este. Por ejemplo, desde principio teníamos claro que la terminología sería uno de los puntos fuertes de este trabajo y, por esa razón, durante todo el proceso tuvimos en mente cómo dotar de una función práctica a nuestro análisis terminológico. Un fichero terminológico especializado es muy útil para establecer conclusiones teóricas, pero se convierte en algo vivo si convertimos ese fichero en una base terminológica fácil de usar en nuestro día a día como traductores.

Además, establecer unos objetivos de trabajo desde la fase inicial permite sistematizar el trabajo y detectar con gran rapidez la aparición de nuevos objetivos y líneas de investigación futuras, sin perder de vista el punto de partida.

2. CONTEXTUALIZACIÓN LINGÜÍSTICA

En este capítulo comenzaremos por ofrecer una contextualización lingüística del texto objeto de análisis, es decir, explicaremos a qué tipo de texto nos enfrentamos y cuáles son sus características fundamentales; para ello, repasaremos los principales rasgos de los textos científico-técnicos y de los textos didácticos. A continuación, de forma más concreta, revisaremos cuáles son las características específicas de los manuales técnicos y de los manuales de seguridad informática.

Hemos de tener en cuenta que los textos no son entes aislados, ya que forman parte una realidad tangible, de un campo del saber, de una tipología textual, de un registro lingüístico, de un tono y que están redactados en un idioma específico con todo lo que ello conlleva. Todos estos elementos son determinantes a la hora de analizar las características de un texto.

No podemos olvidar que el contexto representa el escenario en el que se inscriben los textos. Por otra parte, existe una evidente relación de dependencia entre todo texto respecto a otros textos dentro de su tradición cultural (Halliday y Hasan, 1985)[6]; es decir, existe un contexto intelectual de conocimientos adquiridos[7]. Cada lectura de un texto supone una interpretación que pretende recuperar toda la información posible a partir de una amplia gama de significados. El teórico y traductor mexicano Octavio Paz (1990: 22) apuntaba esta idea en *Traducción: Literatura y literalidad*, donde describe la figura del traductor como el ser en que se aúnan cualidades y capacidades propias del intérprete, del crítico y del lector. Adelantó también Paz muchas de

[6] Véase: M. A. K. HALLIDAY y R. HASAN: *Language, Context and Text: Aspects of language in a social semiotic perspective*. Oxford, Oxford University Press, 1985.

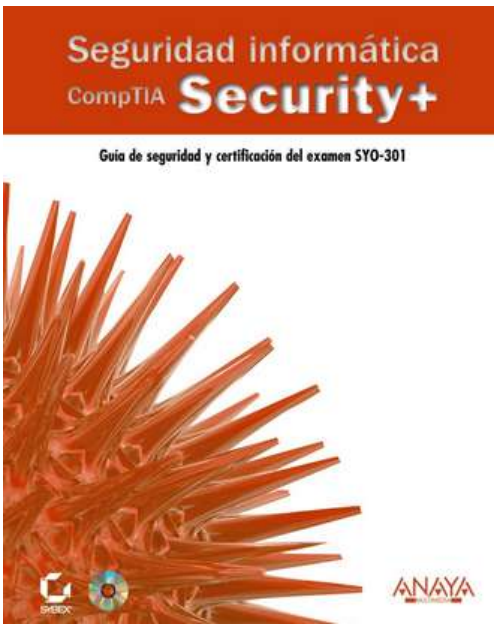
[7] La relación entre el lenguaje y la cultura cobró gran relevancia entre los teóricos de la traducción. Así, Nida (1945: 207) formuló el siguiente principio: "Las palabras no pueden ser comprendidas correctamente separadas de los fenómenos culturales localizados de los cuales son símbolos". El teórico defendía la sociolingüística corno disciplina indispensable en el análisis del texto que traducir y en el mismo proceso de su traducción, incluso en el caso de lenguas pertenecientes a culturas similares o próximas (Nida, 1995: 107). Lingüistas, antropólogos, filósofos y traductores comparten el convencimiento de la importancia del contexto para analizar, explicar, comprender y practicar la comunicación.

las ideas presentes en la semiótica actual al visualizar la labor del traductor como un trabajo sígnico eminentemente cultural.

En el caso de los textos técnicos, una de las prioridades del traductor ha de ser en todo momento ser lo más objetivo y unívoco posible para no ofrecer diversas interpretaciones. Como señalaremos más adelante, esta es una de las características más importantes de los textos científico-técnicos. Es más, se podría decir que esto forma parte de la cultura textual de esta tipología de textos.

Como ya hemos comentado en la introducción, el presente trabajo de investigación se centra en el análisis del libro *Seguridad informática CompTIA Segurity+* publicado por Anaya Multimedia en 2011. Por un lado, hemos realizado un análisis terminológico que nos ha permitido centrarnos en la creación de un fichero terminológico destinado a la creación de una base de datos terminológica para su posterior uso profesional. Por otro lado, hemos profundizado en los pormenores de un proyecto de traducción desde su inicio hasta la publicación del texto final.

Con el fin de ofrecer una contextualización lo más específica posible, a continuación ofrecemos la propia reseña del editor, que encuadra perfectamente el contexto del texto objeto de la investigación.



Reseña del editor

La seguridad informática es un requisito indispensable para todas las empresas. Proteger los sistemas de información, desde el más potente de los servidores, hasta el más pequeño portátil, es esencial para los expertos. Un profundo estudio de los sistemas, las redes, los programas, y hasta el propio hardware es indispensable para prevenir amenazas futuras y eliminar las ya existentes. Esta guía de estudio es un referente a la hora de hacer frente al mundo inseguro que nos rodea. Aporta los conocimientos y habilidades necesarios para disponer de una formación profunda en materia de seguridad. Es ante todo, un recurso para solucionar los retos profesionales. La certificación SY0—301 en materia de seguridad tiene un indudable prestigio profesional. Gracias a este libro, aprenderá todo lo necesario para poder aprobar el examen CompTIA, que le otorgará un valor añadido en el mundo laboral. Las competencias profesionales de estos textos en materia de seguridad son importantes incluso si solo quiere aprender o ponerse al día. El CD-ROM incluido dispone de exámenes y ejemplos completos, así como provechosas herramientas y utilidades provenientes del libro original en inglés.

Como resulta comprensible, abordar el análisis de un texto tan amplio de forma exhaustiva no es tarea fácil. Por lo tanto, y dada su gran extensión (650 páginas), hemos acotado el texto objeto de investigación con el propósito de alcanzar resultados más concretos y específicos. Del total de 15 Capítulos, hemos seleccionado los cinco siguientes:

Capítulo	Título capítulo	Numeración	Nº Páginas
2	**Infraestructura y conectividad**	Páginas 27 a 79	52 págs.
3	**Proteger redes**	Páginas 81 a 119	38 págs.
5	**Control de acceso y gestión de identidad**	Páginas 175 a 205	30 págs.
10	**Seguridad física y basada en hardware**	Páginas 375 a 399	24 págs.
12	**Seguridad de red inalámbrica**	Páginas 429 a 454	25 págs.

Tabla 1. Capítulos seleccionados para el análisis.

Hemos seleccionado un total de 170 páginas de las 650 que constituyen el manual. Esto supone un análisis del 30% del corpus textual, tal como podemos observar en el Gráfico 1. Consideramos que este porcentaje es una muestra representativa de la totalidad de la publicación para los fines del

presente trabajo de investigación. No obstante, en futuras investigaciones abordaremos la ampliación de nuestra base de datos terminológica.

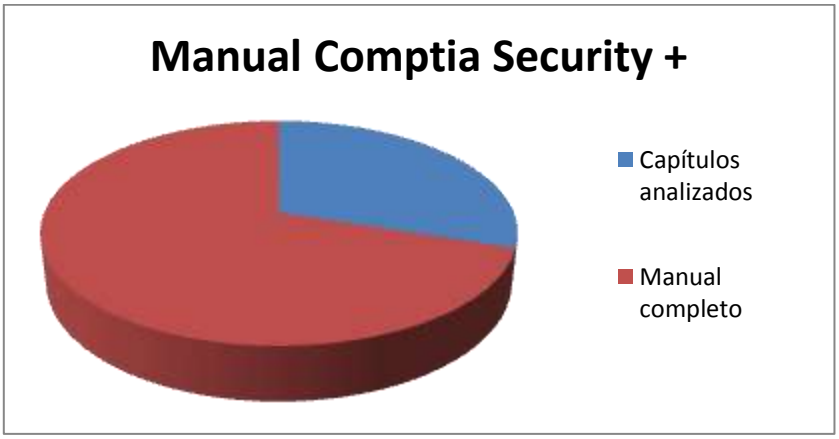


Gráfico 1. Porcentaje de capítulos del manual que constituyen el corpus.

Acotar el texto nos permite realizar un análisis terminológico detallado y documentado, además de facilitar la lectura del presente trabajo de investigación. El proyecto terminológico versará, pues, sobre los términos relevantes hallados en el 30% del extenso manual, lo que consideramos como muestra suficientemente representativa.

Para seleccionar los términos que pasarían a formar parte de la base de datos terminológica, la intuición profesional se une a las posibilidades que ofrecen las herramientas de extracción terminológicas.

En un apartado posterior del presente trabajo de investigación se explica de forma pormenorizada el proceso de extracción terminológica y las herramientas empleadas[8] para tal fin; así describiremos algunas de las herramientas de extracción terminológica más conocidas y explicamos qué pasos hemos seguido para seleccionar los términos (frecuencia de aparición, grado de especialización, etc.). En nuestro caso, hemos utilizado AntConc, uno de los programas de extracción terminológica de uso más frecuente debido a los buenos resultados que ofrece.

Por su parte, la selección de estos capítulos se basa en la densidad terminológica de los mismos, es decir, en la cantidad de términos que aparecen

[8] Véase el apartado: 3.4.2.2 AntConc.

en el texto, que está condicionada por el tipo de discurso. En este caso, nos encontramos ante un texto híbrido con componentes de diversa índole en el que destacan las siguientes características:

- **Discurso especializado:** dirigido a especialistas (existen distintos grados de especialización).
- **Discurso didáctico:** destinado a la formación.
- **Discurso divulgativo:** enfocado hacia el público general.

El número de términos utilizados difiere habitualmente entre estos tres tipos de discurso. Los niveles de competencia en cuanto a la temática tratada en las producciones lingüísticas se reflejarán en el mayor o menor uso de terminologías específicas (Condamines, 1993). De este modo, la comunicación especializada requiere que la terminología se adapte a cada género discursivo, el cual viene determinado por la cantidad de información compartida entre emisor y receptor y la finalidad del texto (Marinkovich, 2006).

La densidad terminológica y el grado de especialización de los términos de un texto dependerán, a fin de cuentas, de la formación de los destinatarios del texto y de la finalidad de ese texto. Así pues, no encontraremos el mismo número de términos ni el mismo grado de especialización en el contenido del Título I del Libro II del *Código Penal español* ("Del homicidio y sus formas") y en una noticia de un periódico en la que se relata un homicidio[9].

La selección de una fuente que sirviera para extraer el corpus textual objeto de análisis en este estudio no ha sido casual (Dubuc y Lauriston, 1997: 85). Para ello, atendimos a dos directrices básicas:

1. Por un lado, tuvimos en cuenta la adecuación de la fuente textual, de forma que reflejara situaciones de comunicación diferentes dentro del discurso de contenido especializado.

2. Por otro, consideramos la idoneidad de la fuente al ámbito de estudio: los textos han de ser fieles a los parámetros de cohesión, coherencia,

[9] Véase también:
M. SEVILLA MÚÑOZ, Y E. MACÍAS OTÓN: *Terminología. Módulo I: Introducción a la terminología. OpenCourseWare*. Universidad de Murcia, 2008.
URL: <http://ocw.um.es/cc.-sociales/terminologia/material-de-clase-1/modulo-i.pdf>
[Fecha de consulta: 14 de diciembre, 2016]

intencionalidad, aceptabilidad, informatividad, situacionalidad e intertextualidad (Hartmann, 1987).

Cabe destacar que, de acuerdo con Sinclair (1991), un factor prioritario para la elección de la fuente de estudio es la actualidad del corpus. En este caso concreto, el ámbito de la seguridad informática es un campo del conocimiento que no solo es de plena actualidad, sino que además está en pleno desarrollo y cambia con gran rapidez.

El trabajo terminológico orientado a la traducción debe utilizar como corpus tanto textos originales como traducciones. Esto favorece la investigación sobre los patrones preferidos por una determinada comunidad a la hora de traducir, a la vez que se posibilitará la identificación de áreas problemáticas de traducción dentro del dominio de la seguridad informática. Para la elaboración del proyecto terminológico hemos intentado que nuestro corpus sea equilibrado, es decir, que la información utilizada esté equilibrada entre las dos lenguas y que cubra todos los contextos comunicativos que hemos estimado significativos. Sin embargo, la tarea no ha carecido de dificultades: el hecho de que el inglés se imponga en la seguridad informática, así en otras especialidades informáticas, como *lingua franca* ha dificultado la labor de encontrar textos especializados redactados originalmente en español. Además, en lo que se refiere a textos destinados al lego, hemos detectado muchos en inglés, pero pocos en español. El material extraído de internet para la información del lego ha sido sustancial en inglés y muy escaso en español.

Para elegir los capítulos nos hemos centrado en aquellos que mejor ejemplifican una doble validez (Tercedor Sánchez, 1999). En primer lugar, optamos por una validez traductológica, que muestre la mayor variedad de situaciones y contextos comunicativos posible, algo que nos permitirá analizar distintas estrategias de traducción (calcos, préstamos, neologismos, etc.) e investigar cuáles son las principales dificultades que encuentra el traductor especializado y cómo las aborda. Por otro lado, buscamos la validez terminológica, por lo que elegimos una fuente que recibió una revisión técnica por expertos en el dominio, sobre todo en lo que se refiere a la utilización real de los términos por parte de los especialistas y a la ponderación de las fuentes bibliográficas utilizadas.

Como explica Cabré (2002), las consecuencias del estudio de la terminología de especialidad en su contexto comunicativo nos permiten

analizar la influencia que esta ciencia recibe desde otros ámbitos del conocimiento en su contacto con otras especialidades científicas y como resultado de su utilización por otros profesionales, que pueden concretarse en tres aspectos.

1. **Aspectos Cognitivos:** Debido al cuestionamiento de la uniformidad e independencia de la terminología especializada con el fin de defender la integración cognitiva diversificada en función de los hablantes. El traductor especializado adquiere nuevos aspectos cognitivos específicos del campo del saber con el que trabaja. Por ejemplo, un traductor jurídico debe conocer los aspectos cognitivos asociados a los términos especializados de su materia (derecho de la empresa, derecho civil…). No es lo mismo redactar textos jurídicos que informes médicos, ya que cada tipología textual tiene asociados unos aspectos cognitivos idiosincrásicos que la hacen única. De ahí es tan importante el domino de las herramientas terminológicas por parte del traductor especializado, ya que le ayudan a estructurar los conocimientos adquiridos para poder utilizarlos y reutilizarlos en su práctica profesional de forma útil y eficaz.

2. **Aspectos Lingüísticos:** Dado que se rechaza el concepto del término especializado como elemento aislado del concepto general. De este modo, se acepta que forme parte de la competencia de los hablantes en la medida en que adquieren con cocimientos especializados. Los términos no son elementos aislados, ya que su uso depende del nivel de conocimiento del hablante. El traductor especializado adquiere unas competencias lingüísticas específicas del campo del saber con el que trabaja (por ejemplo, derecho, seguridad informática, automoción, medicina, marketing, finanzas…) que le permiten tener un conocimiento avanzado y profundo de los términos con los que trabaja y sus características. Surge aquí una cuestión muy interesante: ¿debe el traductor especializado ser un experto en la materia sobre la que traduce?, es decir, ¿un traductor jurídico debe ser abogado? o ¿un traductor de textos sobre seguridad informática debe ser un informático? Está claro que, como mínimo, el traductor especializado debe ser un gran conocedor de la materia con la que trabaja.

3. **Aspectos Sociales:** Porque el estudio de los términos en su contexto comunicativo cuestiona el planteamiento de la terminología prescriptiva de la univocidad entre concepto y término y defiende que la variación

discursiva que surge del contexto comunicativo en que se produce presenta, en ocasiones, variaciones cognitivas significativas. Esto depende en gran medida del ámbito del saber con el que trabajemos, por ejemplo, una de las principales características de los términos médicos es su univocidad en contraposición a algunas siglas o acrónimos del ámbito informático como MAC[10].

En términos generales este trabajo se enmarca en el ámbito de la traducción especializada y de la terminología aplicada. Más concretamente, podríamos afirmar, sin lugar a dudas, que el manual seleccionado es un texto científico-técnico de carácter didáctico. Por lo tanto, también podemos ubicarlo dentro de los textos de carácter híbrido, dada su doble naturaleza. Por esta razón, el capítulo 2 de este trabajo de investigación se dedica a describir brevemente las características de la traducción especializada, la traducción técnica[11], así como de la tipología del corpus. El recorrido de lo general a lo particular nos permite ilustrar el contexto del trabajo.

2.1 La traducción especializada

En contraposición a la traducción de textos de carácter general, la traducción especializada requiere la adquisición de unas habilidades más avanzadas dado su mayor grado de especificidad. El traductor especializado no solo debe poseer un conocimiento lingüístico, sino que debe contar con un conocimiento del campo de especialidad. Además, en todo caso será necesaria una búsqueda documental que sirva de apoyo a la labor de traducción. Es ahí donde serían necesarias herramientas terminológicas como las que son objeto de estudio en este trabajo.

A lo largo de su experiencia profesional, la autora de este trabajo ha podido comprobar cómo cada texto tiene sus propias peculiaridades y grados de especificidad. De hecho, se podría decir que la mayor parte de textos a los

[10] MAC: Véase MAC (*Media Access Control,* Control de acceso a medios), MAC (*Mandatory Access Control,* Control de acceso obligatorio) y MAC *(Message Authentication Code,* Código de autenticación de mensaje).

[11] Véase: S. GAMERO: *Introducción a la traducción técnica*. Jaén, Editorial Ariel, S.A., 2005.
URL: <http://www3.uji.es/~gamero/traductortecnico.pdf>
[Fecha de consulta: 14 de diciembre, 2016]

que se enfrenta un traductor profesional son especializados en diversa medida. Por otra parte, el estudio del mundo laboral de la traducción aporta información sobre los campos de especialidad y los tipos de textos más demandados por el cliente.

Dentro de los textos especializados podemos encontrar distintos rasgos distintivos que los caracterizan y los incluyen dentro de un tipo de especialización determinado. A su vez, cada tipología cuenta con sus propias estructuras, convenciones, terminología y grados de especificidad. Por esta razón distinguimos distintas variedades de textos especializados y ámbitos de traducción: ámbito jurídico-económico, traducción científico-técnica o traducción audiovisual, entre otras. El cuadro que aparece a continuación resume los tipos de traducción de especialidad, así como las tipologías textuales que engloban cada uno de ellos y el sector profesional al que pertenecen.

TRADUCCIÓN ESPECIALIZADA	TIPO DE TEXTO	SECTOR
Jurídico-Económica	Sentencias, directivas, normativas, contratos, circulares, facturas, albaranes, seguros, etc.	Tribunales de justicia, administraciones públicas, organizaciones internacionales, empresas, departamentos de comercio exterior, abogacía, etc.
Científico-Técnica	Historiales clínicos, manuales de instrucciones, guías de uso, prospectos, ensayos clínicos, artículos científicos, etc.	Hospitales, empresas farmacéuticas, empresas de automoción, laboratorios clínicos, etc.
Literario-Humanística	Textos poéticos, textos narrativos, textos dramáticos, folletos turísticos, textos periodísticos, textos de divulgación cultural, etc.	Editoriales, empresas turísticas (agencias de viajes, hoteles, etc.), departamentos de redacción, etc.
Audiovisual	Guiones cinematográficos, películas, documentales, dibujos animados, software, productos multimedia, etc.	Estudios de doblaje, empresas del ámbito audiovisual, cine, televisión, empresas del sector informático, etc.

Tabla 2. Los tipos de traducción de especialidad.

2.1.1 Lenguaje especializado. Características de las lenguas de especialidad

En la obra *La terminología: teoría, metodología y aplicaciones*, Mª Teresa Cabré ofrece una definición de lengua general y de lenguaje de especialidad. Para esta autora (1993: 127ss), una lengua general está constituida por un conjunto diverso de subcódigos que los hablantes utilizan "en función de sus modalidades dialectales", seleccionándolos según las necesidades expresivas y de las características particulares del contexto comunicativo en el que se encuentran. Junto a ellos, que hacen que la lengua sea compleja y que tenga múltiples variedades, toda lengua general está formada por un conjunto de reglas y unidades (fonológicas, morfológicas, semánticas y pragmáticas) comunes a todos los hablantes.

Por otro lado, los lenguajes de especialidad, según Cabré (1993: 129), son un "conjunto de subcódigos -parcialmente coincidentes con el subcódigo de la lengua común- caracterizados en virtud de unas peculiaridades "especiales"". Estas características son propias de cada lenguaje de especialidad, ya sea por la temática, el tipo de interlocutores, la situación comunicativa o la intención del hablante entre otros.

En la comunicación especializada las funciones de representación y transferencia del pensamiento especializado tienen dos niveles distintos de actuación: el real y el estandarizado. El conocimiento real está sesgado culturalmente y la comunicación se desarrolla también en situaciones reales que rompen con el esquema de comunicación clásico de especialista a especialista, e incluyen, entre otros, el discurso didáctico o el divulgativo. Así, los conceptos de niveles de abstracción, grados de especialización o densidad terminológica adquieren un papel de primer orden en esta propuesta. En cuanto a la representación y comunicación especializada estandarizadas, estas son fruto de un esquema creado semi-artificialmente por consenso. Es en este esquema en el que las características atribuidas a la terminología, de univocidad y ausencia de ambigüedad y polisemia, se dan en toda su extensión (Cabré, 2000: 11). Como veremos estamos hablando de los dos enfoques típicos del trabajo terminográfico: el descriptivo y el prescriptivo.

Partiendo de estos aspectos, Cabré (1997b: 15) formula el Principio de la Variación a partir del cual se derivan gran parte de los fundamentos de la Teoría Comunicativa de la Terminología:

> La comunicación conlleva inherentemente la variación, explicitada en formas alternativas de denominación del mismo concepto (sinonimia) o en apertura significativa de una misma forma (polisemia). Este principio es universal para las unidades terminológicas, si bien admite diferentes grados según las condiciones de la situación comunicativa. El grado máximo de variación de la terminología lo cumplirían los términos de las áreas más banalizadas del saber y los que se utilizarían en el discurso de registro comunicativo de divulgación de la ciencia y de la técnica; el grado mínimo de la variación sería propio de la terminología normalizada por comisiones de expertos; el grado intermedio, la terminología usada en la comunicación natural entre especialistas.

2.2 La traducción científico-técnica

A la hora de describir las características que presenta la traducción científico-técnica no podemos olvidar que siempre van a estar en función de la naturaleza particular de cada texto. No obstante, el abanico de textos de este ámbito es muy amplio y, dentro de la categoría de textos científico-técnicos, encontramos textos jurídicos, informáticos, médicos, mecánicos, literarios, matemáticos, físicos, etc. La cantidad de tipologías textuales está ligada a cada una de las áreas que existen, por lo que hay tantos tipos de textos como áreas de conocimiento.

Las mayores dificultades a las que se enfrenta un traductor científico-técnico son generalmente léxicas. En áreas como la informática, en ocasiones, resulta complejo hallar la denominación para los conceptos. Por ejemplo, hay entidades como Microsoft que sacan al mercado las últimas innovaciones y hay que, literalmente, “inventar” un nuevo término, siempre aplicando la lógica y teniendo en cuenta que con dicho nombre se pasará a conocer dicha idea o producto. Sin embargo, también habrá expresiones que ya se habrán empezado a utilizar antes de que se inicie el proceso de traducción, con lo que la única opción será mantener el término tal y como se esté ya utilizando (casi siempre en inglés).

Una vez que se ha tenido en cuenta todo esto, no hay que olvidar que el traductor científico-técnico no es del todo libre a la hora de traducir, ya que en muchas ocasiones es el propio cliente el que establece sus propias normas de traducción, que no solo incluyen el formato, sino también vocabulario y normas para la gramática del texto.

En un nivel más técnico, según Maillot (1969, 1981), la traducción de textos científico-técnicos exige una precisión y un rigor que no se puede comparar con la de un texto literario o periodístico. Esto se debe a que su principal objetivo es la transmisión de información y datos con la mayor simpleza posible. Por esta razón, las equivalencias científicas o técnicas tienen que ser unívocas y exactas sin ningún tipo de ambigüedad.

Una de las características de la traducción científico-técnica es la utilización de un discurso universal determinado por la normalización lingüística de términos para alcanzar la mayor objetividad posible por parte del traductor. Sin lugar a dudas, la *lingua franca* de los textos científico-técnicos es el inglés y, por lo tanto, la mayor parte de los neologismos que aparecen en ellos proceden de esta lengua. Es por todo esto que los textos científico-técnicos se caracterizan por la escasa presencia, o total ausencia, de la función expresiva.

Algunos de los sectores de la traducción científico-técnica son la medicina, la investigación, la tecnología, las ingenierías, las nuevas tecnologías, etc. En nuestro caso concreto, trabajamos con un texto sobre seguridad informática. Puesto que el uso lingüístico en los textos está determinado por el género o la situación comunicativa concreta, concederemos una especial importancia al análisis lingüístico de nuestro corpus. En el siguiente apartado nos detenemos, también, en las características propias del lenguaje científico-técnico.

2.3. Tipología del corpus

El corpus objeto de análisis en este trabajo, en concreto los cinco principales capítulos del manual *Seguridad informática CompTIA Segurity* +, se engloba dentro del ámbito de la informática, una de las áreas que forman el variado y cambiante grupo de las ciencias informáticas, y de forma más

específica se relaciona con la seguridad informática. Dada su temática podemos afirmar que se trata de un texto científico-técnico. No obstante, la mera observación del manual revela elementos típicamente didácticos, como los resúmenes, los objetivos de examen o las pruebas de evaluación. Todo ello nos lleva a calificar el manual como un texto híbrido, ya que cuenta con rasgos de los documentos científico-técnicos y didácticos.

Aunque la línea divisoria entre los textos didácticos y los científico-técnicos suele ser difícil de establecer, en este caso queda clara desde el principio porque el propio manual describe su propósito formativo y los objetivos que se tratan de cara al examen.

2.3.1 Características generales de los textos científico-técnicos

Por lo general, los textos científico-técnicos poseen las siguientes características:

- Se dirigen a un público especializado ya sea por cuestiones de necesidad o de interés personal.
- Suelen ser muy objetivos, ya que describen una realidad determinada.
- Normalmente no necesitan de recursos estilísticos y van escritos con las palabras necesarias utilizando un léxico especializado.
- Su ortografía puede presentar ciertas peculiaridades (textos químicos, médicos, analíticas, etc.), como el uso de acrónimos y abreviaturas.
- La densidad terminológica de siglas y acrónimos en el corpus seleccionado es especialmente alta[12].
- Se pueden localizar en revistas y libros especializados.
- Existen grandes lagunas léxicas debido a que, en la mayoría de las ocasiones, los avances van más rápidos que las propias traducciones y ciertas culturas no conocen esos avances.

[12] Véase: Proyecto terminológico. Capítulo 6.

- Es muy frecuente que existan limitaciones de espacio a la hora de traducirlos, como en el caso de la informática.

Quizá el rasgo que en mayor grado distingue al lenguaje técnico y científico es el léxico, que no se dirige a personas que no estén familiarizadas con el campo de estudio ni admite distintos grados de comprensión. El vocabulario técnico y científico, en principio, no admite la sinonimia; es necesario un significante propio para cada significado. De esta forma, solo los expertos de una materia podrán distinguir con exactitud los términos propios de su ciencia, pues, aunque puedan existir dichas palabras en la lengua general, en el campo técnico y científico suelen tener un significado unívoco para su uso especializado.

Otro rasgo diferenciador del lenguaje técnico y científico es su universalidad y, por lo tanto, su objetividad, lo que supone que se tiende a excluir la connotación así como los sentidos figurados. El lenguaje científico y técnico debe ser claro y preciso, facilitando una definición exacta de la realidad mediante sus propias definiciones y la presentación clara de conceptos o formulación de hipótesis. La claridad[13] es evidente por el uso de oraciones coordinadas y yuxtapuestas, que se prefieren sobre la subordinación, si bien las subordinadas adjetivas explicativas son frecuentes ya que actúan como aclaración de sus antecedentes. Cabe destacar también el uso de incisos, aposiciones y enunciados parentéticos, así como la repetición de palabras debido a su valor clarificador.

Por otra parte, en español predomina el uso de oraciones impersonales con el fin de dotar al texto de una mayor objetividad. No se suelen utilizar elementos valorativos, ya que se prefieren los tecnicismos y los términos monosémicos, al igual que la creación de una terminología propia de gran precisión. En el caso de una descripción de carácter pragmático de este tipo de lenguaje especializado no podemos obviar que se exige el conocimiento previo del tema, requiere una organización y planificación previa y se utiliza fundamentalmente de forma escrita.

Con todo, el vocabulario científico y técnico se nutre en gran medida de palabras ya existentes del lenguaje general, si bien es cierto que con mayor

[13] Véase también:
J. M.WILLIAMS: *Style: Ten Lessons in Clarity and Grace* (3rd ed.). Boston: Scott, Foresman and Company, 1989.

frecuencia la lengua inglesa se está afianzando como *lingua franca*. Esto supone una ingente cantidad de préstamos y neologismos que el especialista y el traductor han de conocer.

Dado el gran volumen de proyectos de traducción centrados en el extenso campo del ámbito científico-técnico, hay multitud de autores que han analizado tanto las características generales de los textos científico-técnicos, como el tipo de lenguaje que se emplea en esta tipología textual.[14]

El análisis del lenguaje propio del texto técnico o profesional nos revela que su registro está en un nivel intermedio del lenguaje culto y el coloquial, ya que su objetivo no es deslumbrar al lector, sino transmitir una información de forma directa. Las pautas que han de regir los textos técnicos y profesionales son las que aparecen a continuación: claridad (el lector entiende la información con facilidad), corrección (respeto estricto de las normas relativas al léxico y a la sintaxis), brevedad y concisión (sin olvidar que nuestro objetivo es que el lector entienda el texto), trato igualitario y no sexista.

Resulta de vital importancia conocer el proceso de elaboración de los textos científico-técnicos. Existen unas preguntas que sirven como guion para redactar estos textos, ya que al responderlas, accederemos al núcleo del proceso previo a la redacción del texto[15]. Estas preguntas son: ¿qué se pretende conseguir con el texto?, ¿quién es el destinatario?, ¿qué información se ha de transmitir para lograr los objetivos?, ¿cómo se debe organizar esa información? Hay que responder a estas preguntas de forma clara y concisa, teniendo en cuenta qué se pretende conseguir con el texto.

Algunos consejos para la redacción de textos científico-técnicos son los siguientes: preferir palabras concretas a expresiones abstractas, elegir

[14] Véase también:

C. BAZERMAN: *Shaping Written Knowledge: The Genre and Activity of the Experimental Article in Science.* Madison, WI: University of Wisconsin Press, 1988.

J. P. BERROU: *Para escribir bien en la empresa. Cómo redactar para ser leído y convencer*. Barcelona: Deusto, 2004.

F. DINTEL: *Cómo escribir textos técnicos o profesionales.* Barcelona: Alba Editorial 2005.

A. FRASER Y G. SANZ PINYOL: *Manual de comunicaciones escritas en la empresa*. Barcelona: Interactiva, 1998.

L. GARCÍA ARETIO (coord.): *Unidades y Guías Didácticas. Orientaciones para su elaboración*. IUED. UNED, 1997.

[15] Existe una extensa bibliografía al respecto. Resulta de interés la lectura de Casamiglia, 2007; Cassany, 1995; Chalmers, 1986; Crosby, 1997; Gil Iriarte, 2006; Girón Alconchel, 1993; Gómez de Enterría, 2002; Gómez Torrego, 2004; Grijelmo, 2004; y Jones, 1965.

palabras de uso común, huir de los circunloquios, optar por la frase corta, limitar el uso de frases impersonales o pasivas, suprimir las redundancias, equilibrar el número de sustantivos y verbos, evitar formulismos, vigilar el abuso de los extranjerismos, usar de forma cuidadosa las siglas y los acrónimos, ser coherentes en el tratamiento.

Cabe destacar la existencia de una gran variedad de textos profesionales, cada uno de ellos con su propia estructura, estilo y contenido. La única peculiaridad que presenta el lenguaje de los textos técnicos y profesionales es el *vocabulario*, ya que incluye multitud de tecnicismos, es decir, palabras monosémicas que definen con una claridad inequívoca el fenómeno que designan. Los principales modos del discurso que utiliza son la exposición y la argumentación.

Los textos técnicos se refieren a las ciencias aplicadas en sus vertientes tecnológicas e industrial. Estas son las que estudian las posibles aplicaciones y derivaciones prácticas de las leyes y los principios generales establecidos por las ciencias experimentales. Es común englobar los textos técnicos y científicos (pertenecen a las ciencias experimentales puras, las cuales estudian las realidades físicas del mundo y se caracterizan por la búsqueda de principios y leyes generales que posean validez universal) en el mismo ámbito y referirse a ellos como texto científico-técnico. Así, pues, a modo de resumen podríamos señalar las siguientes características:

- **Claridad:** Se consigue a través de oraciones bien construidas, ordenadas y sin sobreentendidos. En general los textos técnicos y profesionales suelen mantener una sencillez sintáctica, aunque también existen textos de sintaxis más compleja.

- **Precisión:** No es recomendable emplear la terminología ambigua y la subjetividad, y en su lugar se prefiere el uso de términos unívocos (que tengan un solo significante y significado).

- **Verificabilidad:** Se tiene que poder comprobar en todo momento y lugar la veracidad de los enunciados del texto, ya sea mediante leyes científicas o hipótesis.

- **Universalidad:** Los hechos tratados se comprenden en cualquier parte del mundo por cualquier miembro del grupo al que va dirigido. Para ello se

recurre a una terminología específica que se puede traducir con mucha facilidad de una lengua a otra. Estos términos científicos, también llamados tecnicismos, suelen ser unívocos, ya que designan una única y precisa realidad.

- **Objetividad:** Se le da primacía a los hechos y datos sobre las opiniones y valoraciones subjetivas del autor.

También cabe destacar que en ningún caso el escritor de este tipo de textos debería descuidar la redacción, ya que perjudicaría la transmisión del mensaje al lector y pondría en entredicho su profesionalidad.

2.3.2 Características generales de los textos didácticos

Además de tratarse de un texto científico-técnico, el manual seleccionado también tiene un marcado componente didáctico debido a que su objetivo principal es la preparación de un examen centrado en la seguridad informática. Como tal, es importante incluir en este trabajo de investigación las características generales de los textos didácticos. Entre otros, Pérez Priego (1997) y Gutiérrez Ascencio (2009) resultan de gran utilidad para profundizar en los rasgos de este tipo de textos.

En el grupo de los textos didácticos se incluyen los textos que se usan en las distintas materias y niveles de formación y tienen como finalidad guiar paso a paso hacia un conocimiento determinado.[16]

Los libros didácticos suelen dividirse en unidades, en este caso concreto quince capítulos centrados en distintos aspectos de la seguridad informática. Como ya se ha mencionado con anterioridad, este trabajo realiza el análisis

[16] Véase también:
R. APARICI: *El documento integrado*. URL: <http://usuarios.lycos.es/saraoa/integra.html> [Fecha de consulta: 14 de agosto, 2013]
S. DEDOLME: *Aspectos didácticos a tener en cuenta en la estructuración de materiales impresos*. UNED. URL: <http://seduca.uaemex.mx/prog_dist/curso/edu_dist/uploads/discpedagmde d.pdf> [Fecha de consulta: 14 de agosto, 2013]
F. SANTAMARÍA: *Herramientas colaborativas para la enseñanza usando tecnologías WEB: Redblogs, Redes Sociales, Wikies, Web 2.* 2005. URL: <http://gabinetedeinformatica.net/descargas/herramientas_colaborativas2.pdf> [Fecha de consulta: 14 de agosto, 2013]

más profundo de cinco de ellos: Capítulo 2: "Infraestructura y conectividad", Capítulo 3: "Proteger redes", Capítulo 5: "Control de acceso y gestión de identidad", Capítulo 10: "Seguridad física y basada en hardware", Capítulo 12: "Seguridad de red inalámbrica". Los contenidos se presentan con un lenguaje sencillo, fácil de comprender e incluyen conceptos definidos basados en conocimientos técnicos o científicos. Llevan al lector hacia una finalidad determinada durante el proceso enseñanza-aprendizaje. Incorporan ejemplos, actividades y sugerencias.

Los textos didácticos se consideran instrumentos, herramientas de trabajo que permiten un proceso de construcción y desconstrucción de un universo comunicativo en el que los receptores tienen la posibilidad de asumir otro papel más allá del de reproductores del emisor, es decir, a partir de una serie de instrumentos de base (documentos naturales) los lectores pueden comprender, reflexionar, analizar, asimilar y disentir acerca de la realidad cognitiva que se les ofrece.

Por lo general, el lenguaje didáctico está despojado de recursos literarios complejos, tales como comparaciones, metáforas y adjetivaciones recargadas, sin querer decir con ello que deban suprimirse completamente todos los recursos literarios, porque sí que pueden utilizarse de forma equilibrada y con un propósito pedagógico claro.

2.3.2.1 Principios para la elaboración de textos didácticos

El principio general que se aplica en los textos didácticos es hacer que el lenguaje no sea un obstáculo sino una guía para entender el texto. Por lo tanto, con independencia del contenido que traten, hay textos de difícil y fácil comprensión[17] debido a la redacción y al uso del lenguaje.

De acuerdo con lo que indica Gutiérrez Ascencio (2009), a continuación señalamos una serie de técnicas que ayudan a facilitar la lectura.

[17] Véase también:
A. MEDINA GÓMEZ et al.: "Elementos que facilitan los procesos de comprensión y aprendizaje de textos", en L. García Aretio (ed.): *El material impreso en la enseñanza a distancia. Actas y congresos.* Madrid: UNED, 1997.

- **Indicadores de jerarquización:** Mecanismos lingüísticos o de presentación que permiten diferenciar niveles de importancia en el material escrito. Entre ellas está:

    a. La norma de colocar la idea central en la primera o segunda frase de cada párrafo

    b. El uso de títulos y subtítulos

    c. Los subrayados

    d. Los recuadros de texto

    e. El uso de tipos variables de letra para indicar la importancia de ciertos títulos o frases.

    Detectar si un autor utiliza o no esas técnicas de manera adecuada requiere una revisión muy cuidadosa del texto, por parte del traductor.

- **Ayudas de vocabulario:** Este punto se refiere a glosarios técnicos, definiciones de conceptos incluidas al comienzo de un párrafo y otros mecanismos similares que favorecen la comprensión del material escrito.

- **Redundancia verbal:** La redundancia en el lenguaje consiste en la reiteración discursiva y se puede lograr al parafrasear las ideas importantes, utilizando oraciones distintas, mediante el desarrollo de cada concepto en todos sus aspectos, el uso de ejemplos y las oraciones que relacionan dos o más conceptos. Hay que tener en cuenta que la redundancia es una especie de «arma de doble filo», porque cuando un material es demasiado repetitivo tiende a cansar al lector.

2.3.2.2 Grado de redundancia

El grado de redundancia será inversamente proporcional al nivel de preparación previa del lector. Si este es muy bajo, la redundancia debe ser alta; es decir, los elementos importantes se repetirán una y otra vez. Si se trata de un lector con alto nivel de formación, la redundancia debe ser baja.

- **Resúmenes:** También son elementos de redundancia, pero merecen un tratamiento especial porque cumplen además otras funciones. En general, ayudan a distinguir las ideas esenciales y permiten que el lector verifique si lo aprendido hasta el momento coincide o no con el resumen. Puede haber resúmenes escritos por el autor o resúmenes solicitados al estudiante.

- **Análisis de legibilidad:** Hay ciertas técnicas de escritura que ayudan a la legibilidad del mensaje. Algunas de las más significativas, según Gutiérrez Ascencio (2009), son las siguientes:

    - Uso preferente de oraciones cortas, simples, afirmativas y activas. Estas son más fáciles de comprender que las oraciones complejas o en voz pasiva.

    - El abuso de muchos calificativos y adverbios complica la identificación de la información e implica más esfuerzo para procesarla. Se debe tratar de expresar las ideas de una manera clara y precisa.

    - El tiempo que toma evaluar la veracidad de una oración está más relacionado con su sintaxis que con su verdadero significado; por lo tanto, no se debe complicar la sintaxis.

    - No se deben usar términos poco conocidos cuando haya otros con significado equivalente de uso más frecuente. Por ejemplo, en lugar de decir "teleológico" se debe decir "orientado a metas", en lugar de decir "infraestructura" se debe decir “edificaciones".

    - Se debe tener cuidado con la ambigüedad; las oraciones ambiguas frecuentes no son reconocidas como tales y el lector puede caer en una interpretación errónea.

    - Es mejor escribir como si mantuviese una conversación con el lector, evitando la forma impersonal que resulta monótona.

    - Uso de la siguiente forma de presentación cada vez que sea apropiada:

a. Definir un hecho concepto o principio

b. Presentar uno o más ejemplos

c. Preguntar al lector sobre características o relaciones de ese hecho, concepto o principio

d. Preguntar sobre los ejemplos o pedir nuevos ejemplos

e. Finalmente, tratar de disfrutar escribiendo el material; el participante probablemente disfrutará también de la lectura.

Asimismo, Gutiérrez Ascencio (2009) distingue los tipos de texto didáctico en función de su extensión:

a. LECTURA CORTA

Es un texto didáctico de corta extensión. Características:

- Documento de texto de extensión mínima de tres y máxima de diez páginas de texto.
- Puede contener imágenes, figuras, tablas, gráficas, entre otros elementos de apoyo visual para acompañar el contenido.

b. LECTURA EXTENSA

Es un texto didáctico con un contenido que abarca las siguientes características:

- Documento de texto de extensión superior a diez cuartillas.
- Puede contener imágenes, figuras, tablas, gráficas, entre otros elementos de apoyo visual para acompañar el contenido.

Ambos tipos de lecturas contendrán la siguiente estructura.

a. Portada
b. Presentación
c. Desarrollo
d. Conclusión o resumen
e. Referencias

En este caso, nos encontramos ante una lectura extensa de 650 páginas dividida en 15 capítulos que tratan diversos temas relacionados con la seguridad informática. A lo largo de la lectura podemos encontrar contenidos propios, citas textuales, cuadros, gráficos, imágenes, texto que hace referencia a otras fuentes, resúmenes del contenido propio, etc. Así, pues, todos estos elementos son propios de los textos didácticos.

2.3.3 Características específicas de los manuales técnicos

Un manual técnico, también conocido como Guía o Manual de usuario, es un documento de comunicación especializada destinado a dar asistencia a las personas que utilizan un sistema en particular (en este caso se trata de un campo en particular, la seguridad informática). Por lo general, este documento está redactado por un escritor técnico, como por ejemplo los programadores del sistema o los directores de proyectos implicados en su desarrollo, o el personal técnico, especialmente en las empresas más pequeñas.

Las guías de usuario se asocian con más frecuencia a los productos electrónicos, como ordenadores y programas. La mayoría de las guías de usuario contienen una guía escrita, así como imágenes asociadas. En el caso de las aplicaciones informáticas, es habitual incluir capturas de pantalla que ilustren gráficamente el programa y manuales que a menudo incluyen diagramas sencillos y detallados que describan los pasos que debe realizar el usuario para llevar a cabo las distintas opciones disponibles. El lenguaje utilizado debe ser accesible, dirigido a una audiencia que podrá no entender un lenguaje demasiado técnico. No obstante, hay manuales claramente dirigidos a un lector medianamente especializado, como es el caso de *Seguridad informática CompTIA Segurity+.*

2.3.3.1 Secciones básicas del manual de usuario

Las secciones de un manual de usuario suelen incluir:

- Una página de portada.
- Una página de título.

- Una página de derechos de autor.
- Un prefacio, que contiene detalles de los documentos relacionados y la información sobre cómo navegar por la guía del usuario.
- Una página de contenido.
- Una guía sobre cómo utilizar al menos las principales funciones del sistema, es decir, sus funciones básicas.
- Una sección de solución de problemas que detalla los posibles errores o problemas que pueden surgir, junto con la forma de solucionarlos.
- Una sección de preguntas frecuentes.
- Dónde encontrar más ayuda y datos de contacto.
- Un Glosario y, para documentos más grandes, un Índice.

Los manuales técnicos de la mayoría de las aplicaciones de software suelen incluir todos los contenidos detallados en el apartado anterior. Dada la proliferación actual de productos informáticos, hay gran cantidad de ejemplos de este tipo. Sin embargo, algunos documentos tienen una estructura más fluida con muchos enlaces internos. Esto dependerá del manual en cuestión.

El término 'guía' se suele aplicar a un documento que aborda un aspecto específico de un producto de software. Algunos ejemplos son: *Guía de Instalación* o *Guía de Introducción*.

En algunos sistemas de software empresarial, en los que los grupos de usuarios solo tienen acceso a una parte de la funcionalidad total de la aplicación, es bastante aconsejable preparar una guía de usuario para cada grupo. Un ejemplo de este enfoque puede observarse en la guía *Autodesk Topobase 2010 Help*, que contiene por separado una *Guía del Administrador* y las distintas *Guíasde Usuario*, además de una *Guía para desarrolladores*. Estos manuales son una herramienta valiosa para el entrenamiento en el trabajo.

En su artículo "Comprender y aprender a partir de los textos especializados en español: aproximaciones desde ámbitos técnico-profesionales" (2006: 37)[18], Giovanni Parodi[19] describe algunas aproximaciones al discurso especializado de gran interés:

[18] A. ESCOFET et al. (eds): *Español para fines específicos. Actas del III Congreso Internacional de Español para Fines Específicos*. Utrecht: Instituto Cervantes de Utrecht, 2006, pp. 35-57.

> Sin lugar a dudas, conocer los rasgos lingüísticos característicos de los textos especializados escritos ha constituido un desafío importante para algunos lingüistas durante los últimos años. El resurgimiento de la lingüística del corpus (Bowker & Pearson, 2002; Pérez, 2002; Parodi, 2005b y 2007) junto al desarrollo de herramientas informáticas han traído nuevas formas de abordar indagaciones y comprobar hipótesis, ahora a partir de grandes corpora con textos digitales auténticos. De este modo, los desarrollos de programas computacionales para el español, aunque menos vertiginosos comparativamente con los de otras lenguas, están permitiendo generar un cambio definitivo en cualquier modalidad de lengua.

Por último, podemos concluir que el texto *Seguridad informática compTIA Seguritiy+* comparte la estructura típica de un manual técnico que se han mencionado con anterioridad. Tanto la estructura del texto como los rasgos lingüísticos que lo componen son esenciales para el análisis de la tipología textual y determinar la naturaleza híbrida de este manual. Para ilustrarlo, se ofrece a continuación el esquema de los distintos apartados del mismo:

Estructura del libro:	Estructura de los capítulos:
➢ Dedicatoria	1. ¿Qué objetivos del examen se tratan?
➢ Agradecimientos	2. Título de capítulo
➢ Sobre el autor	3. Breve contextualización
➢ Índice de contenidos	4. Desarrollo
➢ Prólogo: ¿Por qué merece la pena obtener esta certificación?	5. Ejercicios explicativos
➢ Introducción: Consejos para preparar el examen y objetivos	6. Notas aclaratorias
➢ Capítulos 1-15.	7. Resumen
➢ Apéndice A: Contenido del CD-ROM	8. Ideas clave para el examen
➢ Apéndice B: Glosario	9. Prueba de evaluación

[19] Véase también su artículo "La comprensión del discurso especializado escrito en ámbitos técnico-profesionales: ¿Aprendiendo a partir del texto?", *Revista Signos,* 38(58), 2005, pp. 221-267.
Son también de interés las publicaciones de Schroder, 1991; Ciapuscio, 2003; Gotti, 2003; Mogollón, 2003; Parodi, 2004; Parodi y Venegas, 2004; Parodi y Gramajo, 2003.

➢ Índice alfabético	10. Respuestas de la prueba de evaluación

Tabla 3. Estructura general del libro analizado y de los distintos apartados.

2.3.4 Seguridad informática

Ya en la propia introducción del libro se describe el nivel técnico del mismo y se contextualiza dentro del ámbito de la seguridad informática. Dada la útil y significativa información que ofrece al lector para hacerle saber qué tipo de manual tiene en sus manos y dada la información acerca del grado de especialización útil a la hora de realizar el trabajo de traducción, se incluye a continuación parte del texto que hemos traducido.

Introducción

Si se está preparando para presentarse al examen Security+, no cabe ninguna duda de que está interesado en encontrar el máximo de información posible relacionada con la informática y la seguridad física. Cuantos más datos tenga a su disposición y mayor experiencia adquiera, mejor preparado estará para enfrentarse al examen. Esta guía de estudio está redactada con esa idea. El objetivo es proporcionar suficiente materia para cubrir el temario del examen, pero no demasiada y sobrecargarle con información que esté fuera del ámbito de la prueba.

Este libro presenta el material en un nivel técnico intermedio. Todos los conocimientos y experiencia que tenga relación con conceptos de seguridad, sistemas operativos y de aplicación le serán útiles para ser totalmente consciente de los retos a los que se enfrentará como profesional de la seguridad.

Se han incluido cuestiones de repaso al final de cada capítulo para que tenga una idea de las preguntas del examen. Si ya ha trabajado en el campo de la seguridad, es recomendable que compruebe primero las preguntas con el fin de determinar el nivel de sus competencias. A continuación, utilice el libro para cubrir las lagunas de su formación actual. Esta guía de estudio le ayudará a completar su base de conocimiento antes de presentarse al examen.

Si puede responder al 90 por ciento o más de las preguntas de repaso en un capítulo, no dude en pasar a otro. Si, por el contrario, no puede responderlas de forma correcta, reléalo y vuelva a intentarlo. Su puntuación debería mejorar.

…

¿Por qué debería leer este libro?

> *Si quiere adquirir una formación sólida en seguridad informática y su objetivo es prepararse para el examen aprendiendo cómo incrementar y mejorar la seguridad, este es su libro. Encontrará explicaciones claras de los conceptos que necesita asimilar y, además, la ayuda que le permitirá alcanzar el alto nivel de competencia profesional requerido para tener éxito en el campo elegido.*
>
> *Si quiere obtener una certificación, este libro es lo que necesita sin lugar a dudas. No obstante, si solo quiere intentar aprobar el examen sin entender en realidad la seguridad, esta guía de estudio no le resultará útil. Esta obra está escrita para aquellas personas que quieran conocer en profundidad las aptitudes y el conocimiento sobre seguridad informática.*

Como podemos observar, se trata un manual destinado a unos receptores muy concretos, en el que los niveles de conocimiento están claramente establecidos. Esto nos ayudará a enfocar nuestro análisis y poder anticipar, sin lugar a dudas, que la densidad terminológica será muy elevada, como mostraremos en los gráficos finales.

No obstante, también es interesante contextualizar el ámbito de la seguridad informática en general para entender su importancia y el porqué de la publicación de este extenso manual. De hecho, a pesar del tiempo que ha transcurrido desde su publicación, este sigue siendo un tema de plena vigencia y en plena evolución. Es innegable el predominio de las nuevas tecnologías y las redes sociales, por lo que el tema de la seguridad informática es cada vez más importante y recurrente.

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos se han incrementado de un modo alarmante. Esto, unido a la progresiva dependencia de gran parte de las organizaciones hacia sus sistemas de información ha provocado una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad.

La seguridad informática, al igual que ocurre con la que se aplica en otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implica la necesidad de gestión del riesgo. Para ello, se deben evaluar y cuantificar los bienes que se han de proteger y, en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riegos asociados o que los reduzcan hasta niveles manejables (Ramió Aguirre, 2006).

Una vez que evaluamos el valor de los bienes que proteger, lo más habitual es considerar otras medidas más acordes al valor de nuestros bienes. Podríamos pensar en una puerta blindada, un conserje compartido con otros vecinos o incluso un servicio de vigilancia privada basada en sensores, alarmas y acceso telefónico con una central de seguridad. Con una combinación de estas medidas preventivas con otras correctivas como podría ser una póliza de seguro contra robo, alcanzaríamos un nivel de seguridad que podría considerarse adecuado.

En el ámbito de la seguridad informática también se pueden aplicar los principios de la seguridad en el domicilio. Las únicas diferencias aparecen por las particularidades técnicas asociadas a los sistemas informáticos. La seguridad implica proteger alguna entidad frente a un conjunto de riesgos. En este caso concreto, riesgos relacionados con los sistemas informáticos.

Los sistemas informáticos son vulnerables a muchas amenazas que ocasionan daños que resultan en pérdidas considerables. El perjuicio puede variar desde simples errores en el uso de aplicaciones de gestión que comprometan la integridad de los datos, hasta catástrofes que inutilicen la totalidad de los sistemas. Pueden ocasionarse por la actividad de intrusos externos a la organización, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados propios, o por la aparición de eventualidades en general destructivas. Como consecuencia, los efectos de las diversas amenazas pueden ser muy variados. Pueden comprometer la integridad de la información o de los sistemas, degradar la disponibilidad de los servicios o afectar a la confidencialidad de la información. En cualquier caso una correcta gestión de los riesgos debe implicar un profundo conocimiento de las vulnerabilidades de los sistemas y de las amenazas que los pueden explotar. Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costes, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones.

Algunas de las amenazas más frecuentes que toda organización debería tener en cuenta como fuentes de posibles pérdidas son los errores y las omisiones, las intrusiones, los accidentes y los desastres, la lógica maliciosa y, por último, las amenazas a la privacidad de las personas.

Existe un gran abanico de medidas de seguridad que pueden reducir el riesgo de pérdidas debidas a la aparición de incidentes en los sistemas informáticos. Entre ellas encontramos medidas de gestión (planteadas a medio y largo plazo desde un punto de vista estratégico y táctico) y medidas técnicas (cortafuegos, antivirus o sistemas de copias de seguridad).

El manual analizado reúne una extensa y detallada recopilación de información relacionada con la seguridad informática que incluye medidas técnicas, cálculos del riesgo, temas de infraestructura y conectividad, protección de redes, amenazas y vulnerabilidades, control de acceso y gestión de identidad, educación y protección del usuario, sistema operativo y seguridad de aplicación, fundamentos e implementación de la criptografía (Ramió Aguirre, 2006), seguridad física y basada en hardware, seguridad y vulnerabilidad en la red, seguridad de red inalámbrica, recuperación de desastres y respuesta a incidentes, directivas y procedimientos relacionados con la seguridad y administración de seguridad.

3. FUNDAMENTOS TEÓRICOS Y METODOLOGÍA

Este capítulo se dedica a describir los fundamentos teóricos, la metodología y las fases de trabajo que se han llevado a cabo para la traducción y análisis, eminentemente terminológico, del manual *CompTIA Security +.* Por un lado, se describe cuál es la relación entre terminología y traducción, la historia y el desarrollo de la terminología como ámbito del saber o algunos aspectos fundamentales de la lingüística de corpus y sus aplicaciones prácticas. Por otro, se detallan las fases generales de un proyecto de traducción en las que, como ya hemos mencionado con anterioridad, no solo interviene el traductor, sino que también intervienen muchos otros profesionales. Además, establecemos algunas pautas generales para abordar proyectos de traducción de gran envergadura y complejidad o grado de especialización.

Como cabe imaginar, la publicación de un libro es un proceso complejo en el que intervienen muchos profesionales especializados, desde el traductor al editor, el revisor o el jefe de proyecto. Por lo tanto, hemos de entender la traducción como una fase más del proceso. Un proceso holístico y multidisciplinar en el que hay que tener en cuenta múltiples aspectos además de la traducción (revisión, cuestiones técnicas, de diseño, maquetación, testeo, entrega final, seguimiento, etc.).

Todos los proyectos de traducción de esta envergadura son un trabajo de equipo en el que intervienen profesionales de diversa índole entre los que podemos destacar los siguientes: agencia de traducción, jefe de proyecto, revisor, revisor técnico, editoriales y maquetador. Esto nos lleva a destacar la importancia de la cooperación y la comunicación entre todos los profesionales que van a formar parte de un proyecto de traducción, ya que sentar las bases desde el principio nos llevará a unos mejores resultados y a ofrecer un producto final más competitivo, al mismo tiempo que trabajamos de forma más eficiente y anticipamos problemas que puedan surgir durante el proceso. Evidentemente, y de forma más concreta, nos centraremos en las fases del proceso de la traducción directa, que se centra en la actividad del traductor. Puesto que en un epígrafe posterior señalaremos los pormenores del encargo y la hoja de proyecto, el epígrafe actual tratará meramente de los aspectos metodológicos.

Cabe destacar que esta investigación se realiza con posterioridad en el tiempo, ya que el proyecto se llevó a cabo en el año 2011. Esto nos ha permitido reflexionar detenidamente sobre el trabajo realizado, cómo se llevó a cabo, qué problemas se presentaron y de qué tipo, cuáles fueron las estrategias que utilizamos para solventarlos, qué diferencia a un texto híbrido de otro exclusivamente técnico y lo importantes que resultaron para esta autora los conocimientos de terminología a la hora de abordar la traducción de textos especializados. En realidad, este trabajo de investigación ha sido un ejercicio de revisión, análisis y reflexión sobre un trabajo propio.

Esta reflexión a posteriori también ha favorecido la investigación y el análisis de las nuevas herramientas de traducción asistida y extracción terminológica que han salido al mercado para facilitar la tarea del traductor. Está claro que las nuevas tecnologías avanzan mucho en poco tiempo y ofrecen cada vez mayores ventajas y posibilidades para traductores y terminólogos.

A continuación, nos centramos de forma más detallada en las fases generales de un proyecto de traducción. Como es habitual en este trabajo de investigación, partiremos de los aspectos más generales para ir avanzando de forma progresiva hacia aspectos más concretos y específicos con el fin de facilitar la comprensión y la lectura del texto.

3.1 Fase previa a la traducción

Aunque pueda parecer algo muy obvio, todo traductor profesional que se precie sabe lo importante que es realizar unas comprobaciones previas para determinar si un documento es "traducible" o no y si un documento se puede integrar en un programa de traducción asistida o no. Por lo tanto, la primera fase de todo proyecto de traducción debería ser "comprobar la traducibilidad" del documento, es decir, ¿nos han enviado un documento en buenas condiciones apto para su edición y modificación de cara a la traducción, maquetación e integración con programas de traducción asistida? ¿Ha de ser el traductor el encargado de realizar las optimizaciones pertinentes en el documento para que se pueda traducir?

Todas estas pueden parecer cuestiones menores u obvias a primera vista, pero en la práctica profesional pueden agilizar el proceso o, por el contrario, propiciar multitud de dificultades. De hecho, podrían llevar al retraso del proyecto o al no cumplimiento de las fechas de entrega, algo que retrasaría a todo el equipo involucrado en el mismo. Por ello, siempre es recomendable realizar estas comprobaciones y solicitar al cliente un archivo editable o hacerle saber en qué se traducirá esto en términos de tiempo y presupuesto.

Por nuestra parte, creemos que es fundamental implementar estas prácticas recomendadas como fase inicial de cualquier proyecto de traducción con independencia de su tamaño. Obviamente, estas prácticas recomendadas deberían ser un *must* en los proyectos de gran envergadura, ya que resolver todas estas cuestiones en la fase cero del proceso proporciona agilidad y calidad al mismo tiempo.

1. **Análisis previos de los archivos originales.**

   En primer lugar hay que analizar los archivos originales que se van a utilizar para traducir. ¿En qué formato están? ¿Son editables? ¿Son compatibles con las herramientas de extracción y terminológica y de traducción asistida?

   En caso de que haya que implementar mejoras en los archivos, hay que determinar quién se va a encargar de llevarlas a cabo. Esto debe tenerse en cuenta a la hora de establecer tiempos y presupuestos.

   Cuando se trata de traducciones técnicas hay que abordar el tema de la instalación del software necesario para realizar las capturas de pantalla de acuerdo con la interfaz del texto meta. Una vez más cabe preguntarse, ¿quién es el encargado de realizar estas tareas? Contar desde el primer momento con el software en el idioma del texto meta es especialmente útil para realizar nuestra labor terminológica y minimiza en gran medida la aparición de incoherencias entre el texto traducido y las imágenes ilustrativas del manual.

2. **Estimación del trabajo de diseño que es necesario después de la traducción.**

   Como podemos observar en el presente trabajo de investigación, el traductor especializado no solo se limita a traducir y a realizar la labor

terminológica para la creación de la base de datos especializada. Además, el traductor es el encargado de realizar las capturas de pantalla que servirán para ilustrar los procesos técnicos que describe detalladamente el manual. Es aquí donde entra en juego el diseño, la resolución de pantalla, las distintas versiones de software y un largo etcétera de temas técnicos. En todo momento hemos de tener en cuenta la terminología: para las capturas de pantalla de las interfaces, para modificar y diseñar las imágenes, para la traducción de tablas y gráficos, etc. Nuestra base de datos terminológica será el punto de partida para implementar las decisiones a este nivel, es decir, la base de datos terminológica servirá para homogeneizar la terminología en todos los elementos que forman parte de nuestro manual: texto, tablas, gráficos y capturas de pantalla.

3. ¿Qué hacer con las imágenes?

En este proyecto en concreto, hemos de realizar capturas de pantalla de las interfaces correspondientes en español. Para ello, hay que descargar el software necesario y tener en cuenta la terminología que este utiliza de cara a la creación de nuestra base de datos de terminológica. Como ya hemos comentado con anterioridad, nuestra base de datos terminológica ha de ser una herramienta de referencia constante y debe estar en coherencia con todos los elementos gráficos que formarán parte del manual.

4. Usar reglas para decidir qué partes se pueden traducir.

¿Hay texto incrustado en las imágenes y los gráficos? Esto requiere mayor trabajo de edición y diseño. Además, hay que emplear software específico para modificar este tipo de imágenes. A la hora de abarcar un proyecto de traducción de gran envergadura hay que tener en cuenta todas estas cuestiones para ofrecer un resultado de calidad. A veces, podemos encontrar problemas de espacio, ya que por lo general el español suele utilizar expresiones lingüísticas más complejas que el inglés. Si desde un principio establecemos las pautas de actuación para solventar estas cuestiones, obtendremos mejores resultados y una mayor homogeneidad y coherencia. Obviamente, hemos de tener en cuenta las reglas establecidas para crear nuestra base de datos terminológica.

5. Establecer si se van a utilizar herramientas de traducción asistida.

Un aspecto que determinará todo el proceso es decidir si vamos a utilizar herramientas de traducción asistida, por ejemplo, Trados, Omega-T o Memo Q. Lo mejor es acordar con la agencia o con el equipo de traductores qué programa se va a utilizar para evitar futuros problemas de formato. Utilizar herramientas simplifica el proceso y facilita la labor de revisión del texto, pero si no acordamos de antemano qué herramienta vamos a utilizar, podemos encontrar dificultades a la hora de exportar nuestras memorias de traducción a otros formatos. Aunque suele haber solución, muchas veces requiere tiempo y paciencia unificar formatos diferentes.

6. ¿Creación de memorias de traducción?

En el caso de proyectos de traducción especializada de gran envergadura siempre es recomendable la creación de memorias de traducción específicas para el proyecto en cuestión. Esto nos permite agilizar el proceso, pero además también nos ofrece la posibilidad de homogeneizar las estructuras lingüísticas que utilizamos en nuestra redacción, consiguiendo así que la lectura del texto meta sea más ágil y comprensible.

Al tratarse de un texto con fines formativos, la cuestión de la “claridad” es especialmente importante para que los lectores finales entiendan con facilidad el texto a la hora de estudiarlo. Sabemos de antemano que será un texto muy leído y utilizado por los profesionales que se presenten a los exámenes con el fin de obtener las certificaciones, por eso, no hemos de perder de vista la función divulgativa. Por lo tanto, es recomendable evitar a toda costa el uso de dobletes y expresiones complicadas, ya que llevarían a una lectura más densa y compleja. Al contar con una memoria de traducción no introduciremos distintas versiones de una misma expresión o de un mismo concepto.

Además, la creación de memorias de traducción es especialmente útil cuando se trata de actualizar manuales para nuevas ediciones. De esta forma solamente habría que traducir las partes nuevas que se han introducido en el texto, así como adaptar las ilustraciones a las nuevas versiones de software.

Algo fundamental para que nuestro trabajo terminológico cobre sentido y sea realmente útil para la práctica de la traducción profesional es vincular la memoria de traducción al proyecto y a la base de datos terminológica, tal y como ilustran las siguientes figuras. En un apartado posterior, profundizaremos en la vinculación de la base de datos terminológica con Trados 2014.

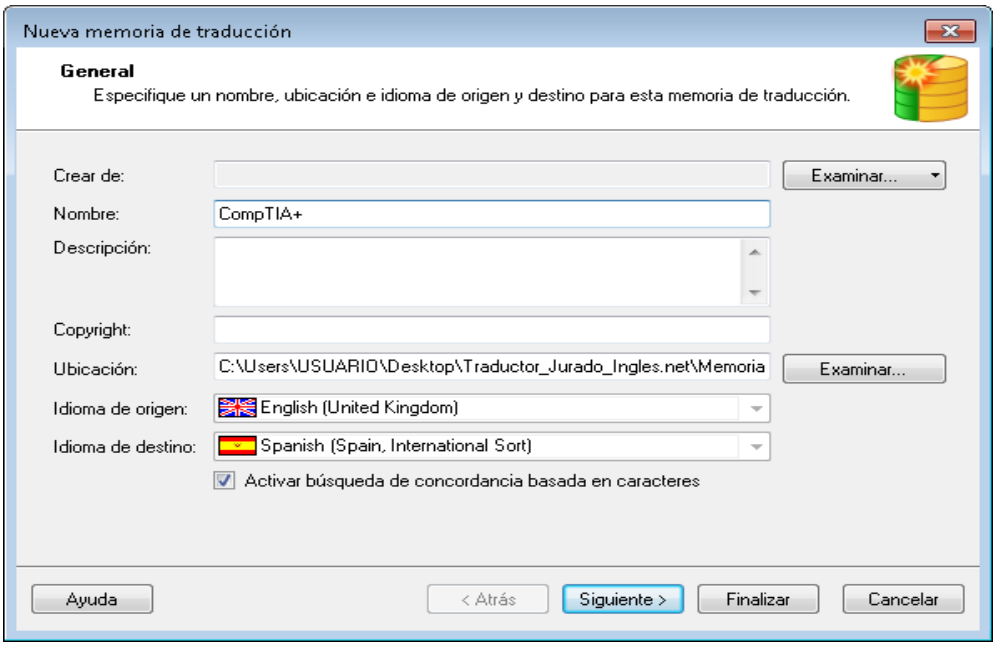


Figura 1. Creación de una memoria de traducción para el proyecto en Trados 2014.

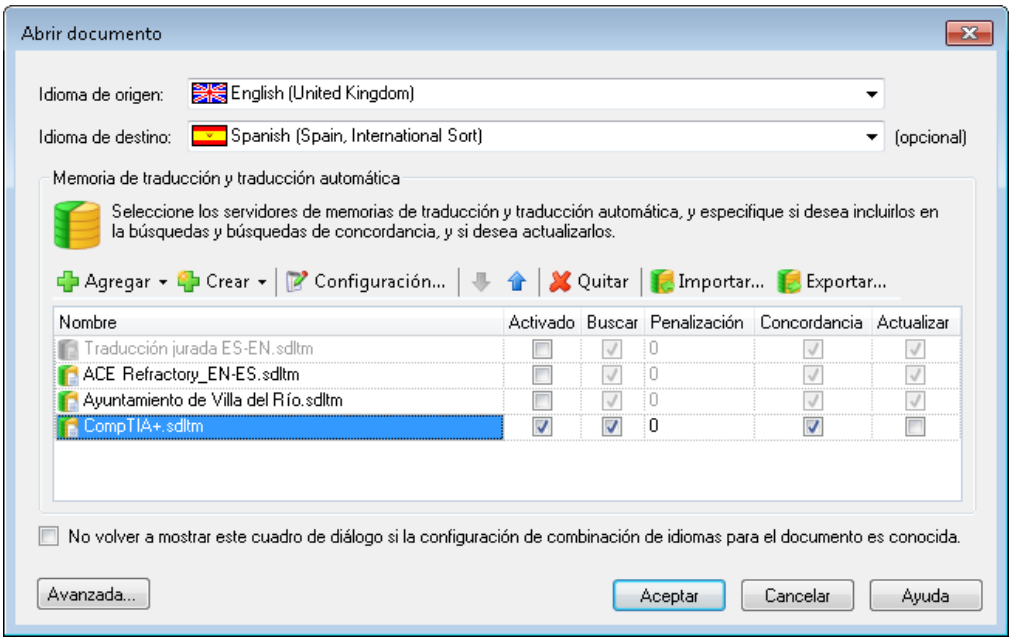


Figura 2. Selección de una memoria de traducción para el proyecto en Trados 2014.

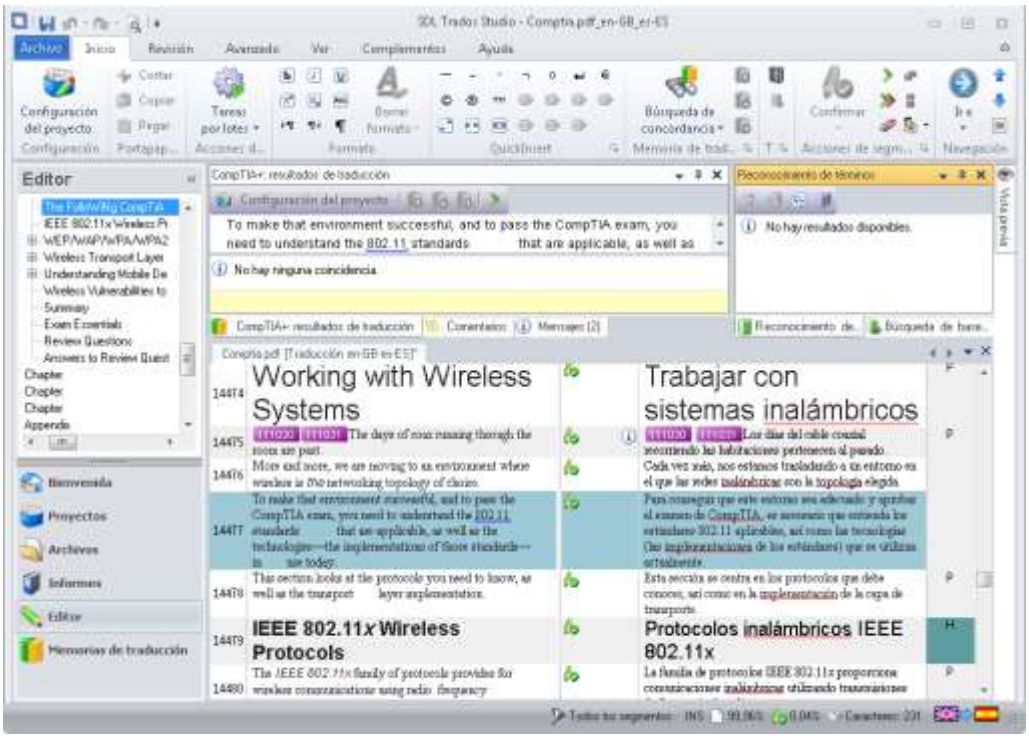


Figura 3. Interfaz de Trados 2014 con el proyecto de traducción abierto y la memoria asociada.

7. Trabajo posterior a la traducción: ¿maquetación?

Dentro del diseño editorial, la maquetación es la encargada de organizar los contenidos textuales (nuestro texto traducido), visuales (capturas de pantalla, gráficos, imágenes, etc.) en forma de libro.

Por lo tanto, una vez realizada la traducción hay que tener en cuenta si el traductor tiene que realizar alguna tarea de maquetación a la hora de configurar el cronograma y el presupuesto. Este no suele ser el caso de proyectos grandes en los que hay un profesional encargado específicamente de ello.

A modo de conclusión, podemos afirmar que el establecimiento de unas pautas de actuación desde el principio no solo simplifica y agiliza el proceso general del encargo de traducción, sino que además evita problemas futuros y nos lleva a ofrecer traducciones de mayor calidad.

Una vez realizado el análisis de todas estas cuestiones generales es el momento de iniciar el proyecto de traducción en sí mismo. En los siguientes epígrafes del presente trabajo de investigación, describimos más a fondo cuáles son las fases generales de un proyecto de traducción.

3.2 Fases generales de un proyecto de traducción

La gestión de proyectos de traducción abarca un gran número de tareas de mayor o menor importancia que pueden marcar de forma decisiva el éxito de un proyecto dado. No hay que olvidar que el traductor autónomo funciona, en realidad, como una empresa unipersonal, por lo que él mismo reúne en su persona todas las funciones que en una empresa cubren distintos individuos con diferentes responsabilidades. Esto quiere decir que en la mayoría de ocasiones será el propio traductor el encargado de realizar las comprobaciones previas al inicio del proyecto de traducción, así como la tarea de traducción propiamente dicha y la de revisión al margen de que el cliente final cuente con sus propios revisores.

Lamentablemente, hoy en día son muchas las agencias de traducción que no tienen en cuenta la importancia de estos aspectos y se limitan a exigir un resultado final sin contemplar cuestiones técnicas ni terminológicas a la hora de establecer plazos y presupuestos. En muchas ocasiones es el propio traductor el que realiza estas tareas sin remuneración y a contrarreloj, lo que, sin duda, no favorece el resultado final.

Por lo tanto, en este caso, el traductor también es responsable de la labor terminológica y de tomar las decisiones que considere oportunas en cuanto a la creación o no de un glosario especializado. Por desgracia, en la actualidad son muy pocas las agencias de traducción que contemplan la fase terminológica en un proyecto de traducción de envergadura en términos de tiempo y presupuesto. Por esta razón, uno de los objetivos de este trabajo de investigación es el de concienciar acerca de la importancia de la terminología en los proyectos de traducción especializada, así como destacar las múltiples ventajas que la terminología puede aportar a todos los actores implicados en el proceso.

Aunque este trabajo de investigación se centra en la actividad traductora, mencionaremos brevemente cuáles han sido todas las fases de trabajo, incluidas las de todos los profesionales involucrados en la realización de este manual.

En líneas generales los proyectos de traducción giran en torno a los siguientes puntos:

1. **Definición del trabajo:** En esta fase se establece el presupuesto con el cliente, se acuerdan los plazos de entrega, se solucionan dudas y se reciben los archivos originales (texto, figuras, fotografías...).

   En la fase de definición del trabajo, hay que escuchar al cliente y preguntar todas las dudas que podamos tener en relación a la traducción y al proyecto en general. No hacerlo se puede traducir en tener que dedicar más tiempo del esperado al proyecto, a la aparición de problemas inesperados (casi siempre técnicos) y a unos resultados que no sean del todo óptimos.

   Este es el momento de hacer preguntas como:

   - ¿Qué es exactamente lo que quiere obtener?
   - ¿Quiere que utilicemos una terminología concreta?
   - ¿Quiere que seamos nosotros los encargados de realizar el trabajo terminológico?
   - ¿Nos va a facilitar acceso a todo el software que necesitamos?
   - ¿Podremos tener acceso a imágenes editables para traducir el texto que contienen?
   - ¿Querrá que le proporcionemos todo el paquete de traducción (memoria de traducción y base de datos terminológica) para futuros proyectos?
   - ¿Hemos de realizar trabajo de maquetación o solo necesita texto simple con etiquetas para que trabaje sobre él el maquetador? Y, si es así, ¿qué tipo de etiquetas quiere que utilicemos?
   - ¿Quiere que nos ciñamos a alguna guía de estilo?

   En resumen, la fase de definición del trabajo sirve para anticipar futuros problemas o dudas que podamos encontrar a lo largo de proyecto. Todas estas preguntas pueden ahorrar mucho tiempo y dinero a los miembros del equipo. Además, son cuestiones esenciales para establecer plazos y presupuestos, ya que si el traductor tiene que dedicar tiempo a realizar otras tareas al margen de la traducción, esto ha de contemplarse en el cronograma del proyecto para cumplir las fechas establecidas. De lo contrario, un proyecto puede acabar siendo un caos y resultará imposible cumplir las fechas de entrega.

2. **Fase previa:** Una vez definido el trabajo que se ha de realizar, el encargo se asigna a un gestor de proyectos, que supervisa en todo momento el proyecto en todas sus etapas (definición, traducción, revisión, corrección, especialistas, edición, maquetación, testeo, entrega final y seguimiento post-traducción).

   Este asigna los archivos de trabajo a un traductor o un equipo de traductores en función de los idiomas de traducción, de la especialidad de traducción y del volumen de traducción. En teoría, es el gestor de proyectos el encargado de coordinar la utilización de la documentación de referencia, glosarios terminológicos, extracción de textos, corpus lingüísticos… Su labor es crucial en esta fase, ya que, si contempla todos estos aspectos, conseguirá una mayor coherencia y cohesión en el texto meta y esto facilitará en gran medida la labor de revisión que se realiza en una fase posterior del proyecto.

   En este caso, como ya hemos señalado, solo hay un traductor autónomo responsable del proyecto. Por lo general, el traductor es el encargado de tomar todas las decisiones en cuanto a la terminología, es decir, él decide si usar herramientas de traducción asistida o no, si realizar una base de datos terminológica o no, si usar glosarios independientes o no, etc. Y, como se desprende de ello, por lo general, las agencias de traducción y los jefes de proyecto no suelen tener en cuenta estos aspectos ni en términos de tiempo, ni de presupuesto. Por lo tanto, en la mayoría de ocasiones, el traductor debe tomar todas estas decisiones y realizar tareas que a veces no son remuneradas.

   Al margen de todas estas cuestiones de índole laboral, la fase previa a la traducción sentará las bases de la fase de traducción propiamente dicha y, si le dedicamos el tiempo que merece a todas estas cuestiones, conseguiremos agilizar mucho las fases posteriores y ganaremos tiempo para dedicarlo a la traducción, al texto y a la redacción, ya que de este modo reducimos al mínimo la posibilidad de que surjan problemas inesperados. Además, gracias a la base de datos terminológica, no dedicaremos tiempo extra a la documentación, puesto que se llevará a cabo una sola vez durante la fase previa a la traducción.

3. **Traducción:** Una vez definido el proyecto y consideradas las cuestiones previas a la traducción, el traductor especializado se encarga de realizar la traducción del proyecto utilizando el material de referencia y la

terminología más adecuada. En este caso, la traducción se lleva a cabo con posterioridad a la realización de la base de datos terminológica, por lo que ya no es necesario realizar búsquedas documentales salvo en algún caso aislado. Esto agiliza el proceso y permite al traductor especializado centrarse por completo en la redacción en sí misma.

Los objetivos son ofrecer una redacción clara y fácil de entender, así como una terminología cohesionada y coherente que no incluya dobles traducciones con fin de facilitar la lectura y la comprensión del texto.

El hecho de utilizar una base de datos terminológica simplifica en gran medida el proceso de traducción, porque, aunque la búsqueda documental y elección de la equivalencia se realiza una vez, el uso de esa equivalencia del término se empleará siempre que este aparezca en el texto (recordemos que estamos ante un texto técnico de equivalencias claramente unívocas). Esto nos lleva a resultados de gran calidad y unicidad, a textos coherentes y cohesionados que no incluyan distintas traducciones para un mismo término generando problemas de comprensión en el lector y duplicidad de conceptos especializados. Pero además, todo esto facilita la siguiente fase del proceso, es decir, la revisión.

4. **Revisión, corrección, especialistas:** Una vez traducidos el texto y las imágenes que este incluye, es el momento de revisar el trabajo realizado. En esta fase intervienen los revisores, correctores de estilo y especialistas terminológicos de acuerdo con las necesidades de cada proyecto. En nuestro caso, al tratarse de un manual técnico especializado con fines divulgativos (y examinatorios) para profesionales del sector de la seguridad informática, se llevan a cabo dos tipos de revisiones, una técnica y otra de estilo, dado el carácter didáctico del texto.

   Como consecuencia de las fases previas, hemos trabajado desde el principio con una base de datos terminológica que ha simplificado el proceso de traducción y revisión, ha reducido al mínimo la introducción de dobles traducciones y favorecido el uso de un lenguaje unívoco y claro, lo que lleva a una lectura más ágil y fácil de entender.

   La fase de revisión es igual de importante que la traducción en sí. Por eso hay que concederle la importancia que se merece. Pero además,

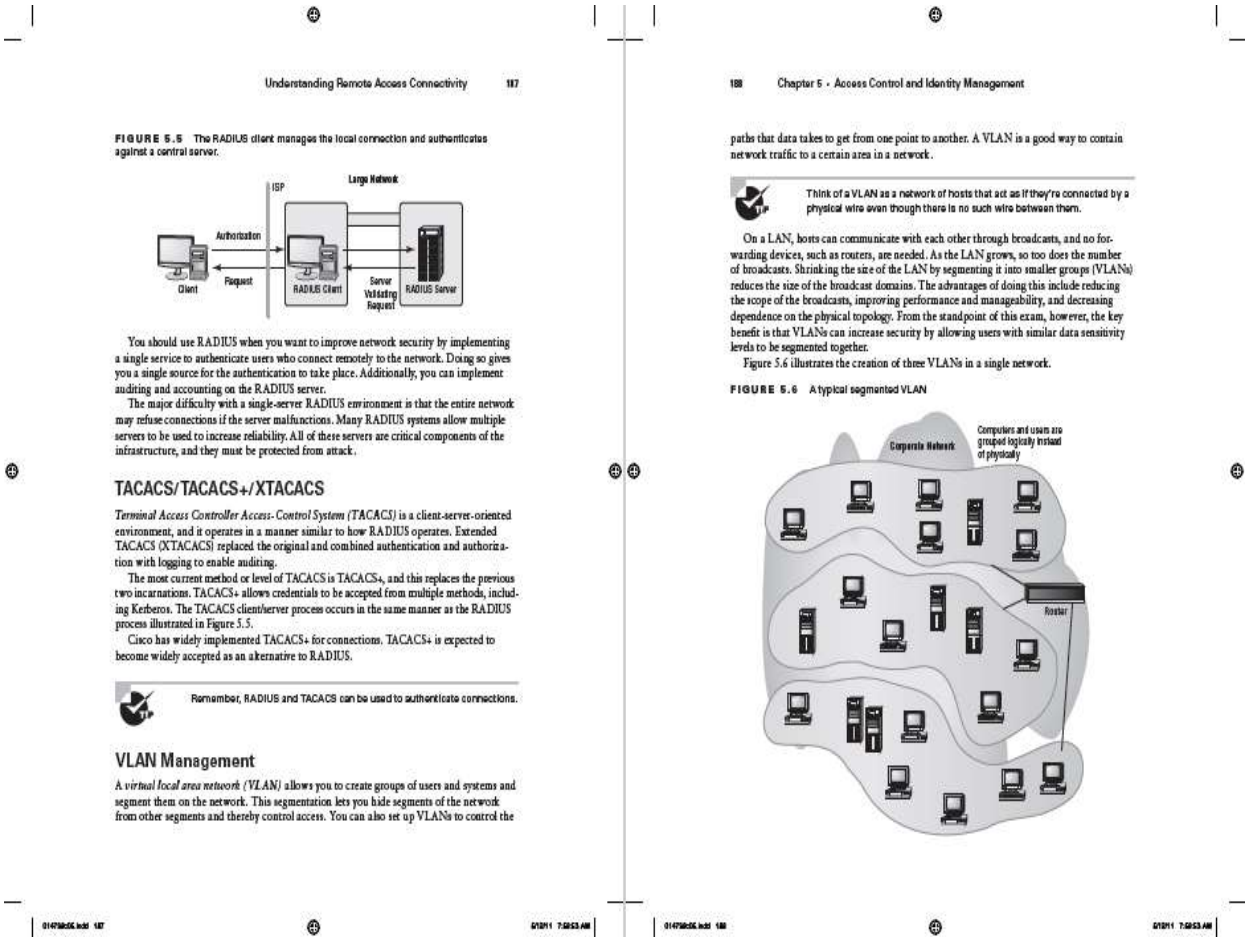
hay que tener en cuenta que se pueden adoptar distintos enfoques a la hora de revisar un texto tan extenso. En este caso, como ya hemos comentado, se realizaron dos revisiones:

a. **Revisión de estilo**: En este tipo de revisión se lleva a cabo un repaso exhaustivo de la redacción, del estilo y de la terminología empleada en términos de exactitud y coherencia.

b. **Revisión terminológica**: Dado que se trata de un manual especializado con fines didácticos, se realizó una revisión terminológica a manos de profesionales del sector para comprobar que la terminología utilizada en la traducción se ajusta realmente a la terminología utilizada en el campo profesional de la seguridad informática. No obstante, al margen de este tipo de revisión, una base de datos terminológica debe basarse en textos reales y documentación actual cien por cien fiable.

5. **Edición, maquetación:** En función del proyecto se requiere editar los trabajos, rediseñarlos o maquetarlos (DTP) de forma que queden listos para su entrega final en el formato acordado o certificados (caso de las traducciones juradas), según sea necesario.

   En este caso, una vez traducidos los textos e imágenes y realizadas las capturas de pantalla en el idioma de destino, el maquetador se encarga de dar forma a todo este material en forma de libro. Para ello debe tener en cuenta factores como el tamaño de página, la tipografía que se va a utilizar o los márgenes.



Understanding Remote Access Connectivity 187

FIGURE 5.5 The RADIUS client manages the local connection and authenticates against a central server.

You should use RADIUS when you want to improve network security by implementing a single service to authenticate users who connect remotely to the network. Doing so gives you a single source for the authentication to take place. Additionally, you can implement auditing and accounting on the RADIUS server.

The major difficulty with a single-server RADIUS environment is that the entire network may refuse connections if the server malfunctions. Many RADIUS systems allow multiple servers to be used to increase reliability. All of these servers are critical components of the infrastructure, and they must be protected from attack.

TACACS/TACACS+/XTACACS

Terminal Access Controller Access-Control System (TACACS) is a client-server-oriented environment, and it operates in a manner similar to how RADIUS operates. Extended TACACS (XTACACS) replaced the original and combined authentication and authorization with logging to enable auditing.

The most current method or level of TACACS is TACACS+, and this replaces the previous two incarnations. TACACS+ allows credentials to be accepted from multiple methods, including Kerberos. The TACACS client/server process occurs in the same manner as the RADIUS process illustrated in Figure 5.5.

Cisco has widely implemented TACACS+ for connections. TACACS+ is expected to become widely accepted as an alternative to RADIUS.

Remember, RADIUS and TACACS can be used to authenticate connections.

VLAN Management

A *virtual local area network (VLAN)* allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access. You can also set up VLANs to control the

188 Chapter 5 • Access Control and Identity Management

paths that data takes to get from one point to another. A VLAN is a good way to contain network traffic to a certain area in a network.

Think of a VLAN as a network of hosts that act as if they're connected by a physical wire even though there is no such wire between them.

On a LAN, hosts can communicate with each other through broadcasts, and no forwarding devices, such as routers, are needed. As the LAN grows, so too does the number of broadcasts. Shrinking the size of the LAN by segmenting it into smaller groups (VLANs) reduces the size of the broadcast domains. The advantages of doing this include reducing the scope of the broadcasts, improving performance and manageability, and decreasing dependence on the physical topology. From the standpoint of this exam, however, the key benefit is that VLANs can increase security by allowing users with similar data sensitivity levels to be segmented together.

Figure 5.6 illustrates the creation of three VLANs in a single network.

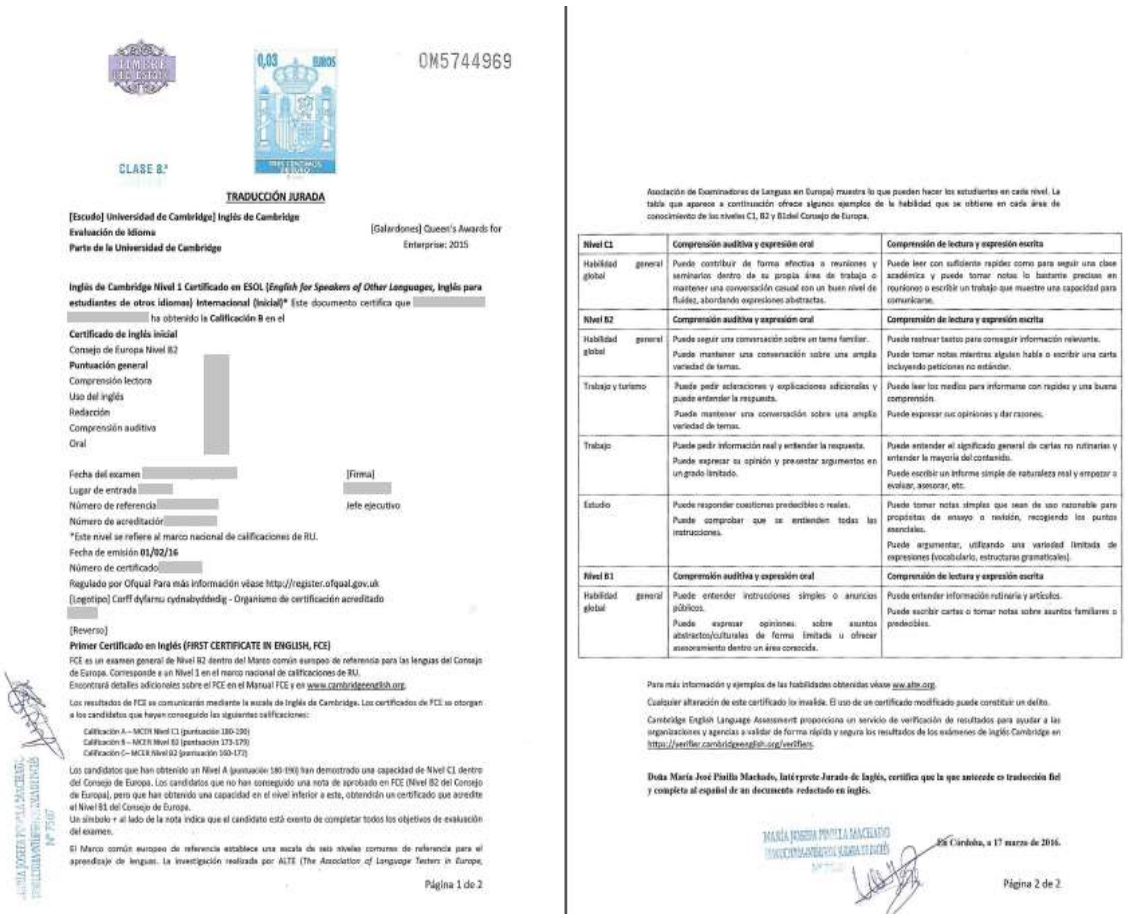
FIGURE 5.6 A typical segmented VLAN

Figura 4. Ejemplo de maquetación del manual original.

Un caso muy distinto es el de las traducciones juradas. Este tipo de traducciones deben reunir unos requisitos formales muy específicos:

- Fórmula en la que el traductor certifica la traducción.
- Sello del traductor-intérprete jurado.
- Firma del traductor-intérprete jurado.
- Es obligatorio adjuntar una copia del original debidamente sellada y firmada en cada una de sus páginas.

Además, una práctica habitual entre los profesionales del sector es imprimir las traducciones juradas en papel timbrado. Como cabe imaginar, en este tipo de proyectos no suele intervenir la figura del maquetador.



TRADUCCIÓN JURADA

[Escudo] Universidad de Cambridge] Inglés de Cambridge
Evaluación de Idioma
Parte de la Universidad de Cambridge

[Galardones] Queen's Awards for Enterprise: 2015

Inglés de Cambridge Nivel 1 Certificado en ESOL (*English for Speakers of Other Languages*, Inglés para estudiantes de otros idiomas) Internacional (Inicial)* Este documento certifica que [redacted] ha obtenido la Calificación B en el

Certificado de Inglés Inicial
Consejo de Europa Nivel B2
Puntuación general
Comprensión lectora
Uso del inglés
Redacción
Comprensión auditiva
Oral

Fecha del examen [redacted] [Firma]
Lugar de entrada [redacted]
Número de referencia [redacted] Jefe ejecutivo
Número de acreditación [redacted]
*Este nivel se refiere al marco nacional de calificaciones de RU.
Fecha de emisión 01/02/16
Número de certificado [redacted]
Regulado por Ofqual Para más información véase http://register.ofqual.gov.uk
[Logotipo] Cerff dyfarnu cydnabyddedig - Organismo de certificación acreditado

(Reverso)
Primer Certificado en Inglés (FIRST CERTIFICATE IN ENGLISH, FCE)
FCE es un examen general de Nivel B2 dentro del Marco común europeo de referencia para las lenguas del Consejo de Europa. Corresponde a un Nivel 1 en el marco nacional de calificaciones de RU.
Encontrará detalles adicionales sobre el FCE en el Manual FCE y en www.cambridgeenglish.org.

Los resultados de FCE se comunicarán mediante la escala de Inglés de Cambridge. Los certificados de FCE se otorgan a los candidatos que hayan conseguido las siguientes calificaciones:

Calificación A – MCER Nivel C1 (puntuación 180-190)
Calificación B – MCER Nivel B2 (puntuación 173-179)
Calificación C – MCER Nivel B2 (puntuación 160-172)

Los candidatos que han obtenido un Nivel A (puntuación 180-190) han demostrado una capacidad de Nivel C1 dentro del Consejo de Europa. Los candidatos que no han conseguido una nota de aprobado en FCE (Nivel B2 del Consejo de Europa), pero que han obtenido una capacidad en el nivel inferior a este, obtendrán un certificado que acredite el Nivel B1 del Consejo de Europa.
Un símbolo + al lado de la nota indica que el candidato está exento de completar todos los objetivos de evaluación del examen.

El Marco común europeo de referencia establece una escala de seis niveles comunes de referencia para el aprendizaje de lenguas. La investigación realizada por ALTE (*The Association of Language Testers in Europe*,

Página 1 de 2

Asociación de Examinadores de Lenguas en Europa) muestra lo que pueden hacer los estudiantes en cada nivel. La tabla que aparece a continuación ofrece algunos ejemplos de la habilidad que se obtiene en cada área de conocimiento de los niveles C1, B2 y B1del Consejo de Europa.

Nivel C1	Comprensión auditiva y expresión oral	Comprensión de lectura y expresión escrita
Habilidad general global	Puede contribuir de forma efectiva a reuniones y seminarios dentro de su propia área de trabajo o mantener una conversación casual con un buen nivel de fluidez, abordando expresiones abstractas.	Puede leer con suficiente rapidez como para seguir una clase académica y puede tomar notas lo bastante precisas en reuniones o escribir un trabajo que muestre una capacidad para comunicarse.
Nivel B2	**Comprensión auditiva y expresión oral**	**Comprensión de lectura y expresión escrita**
Habilidad general global	Puede seguir una conversación sobre un tema familiar. Puede mantener una conversación sobre una amplia variedad de temas.	Puede rastrear textos para conseguir información relevante. Puede tomar notas mientras alguien habla o escribir una carta incluyendo peticiones no estándar.
Trabajo y turismo	Puede pedir aclaraciones y explicaciones adicionales y puede entender la respuesta. Puede mantener una conversación sobre una amplia variedad de temas.	Puede leer los medios para informarse con rapidez y una buena comprensión. Puede expresar sus opiniones y dar razones.
Trabajo	Puede pedir información real y entender la respuesta. Puede expresar su opinión y presentar argumentos en un grado limitado.	Puede entender el significado general de cartas no rutinarias y entender la mayoría del contenido. Puede escribir un informe simple de naturaleza real y empezar a evaluar, asesorar, etc.
Estudio	Puede responder cuestiones predecibles o reales. Puede comprobar que se entienden todas las instrucciones.	Puede tomar notas simples que sean de uso razonable para propósitos de ensayo o revisión, recogiendo los puntos esenciales. Puede argumentar, utilizando una variedad limitada de expresiones (vocabulario, estructuras gramaticales).
Nivel B1	**Comprensión auditiva y expresión oral**	**Comprensión de lectura y expresión escrita**
Habilidad general global	Puede entender instrucciones simples o anuncios públicos. Puede expresar opiniones sobre asuntos abstractos/culturales de forma limitada u ofrecer asesoramiento dentro un área conocida.	Puede entender información rutinaria y artículos. Puede escribir cartas o tomar notas sobre asuntos familiares o predecibles.

Para más información y ejemplos de las habilidades obtenidas véase ww.alte.org.

Cualquier alteración de este certificado lo invalida. El uso de un certificado modificado puede constituir un delito.

Cambridge English Language Assessment proporciona un servicio de verificación de resultados para ayudar a las organizaciones y agencias a validar de forma rápida y segura los resultados de los exámenes de inglés Cambridge en https://verifier.cambridgeenglish.org/verifiers.

Doña María José Pinillo Machado, intérprete Jurado de inglés, certifica que la que antecede es traducción fiel y completa al español de un documento redactado en inglés.

MARÍA JOSEFA PINILLA MACHADO

En Córdoba, a 17 marzo de 2016.

Página 2 de 2

Figura 5. Ejemplo de maquetación de traducción jurada.

6. **Testeo, QA:** Antes de la entrega de los trabajos al cliente se procede a la comprobación de la corrección lingüística de las traducciones, de la ausencia de errores en el proyecto y del correcto funcionamiento del encargo. En el testeo de calidad hay que revisar además la maquetación final del libro, por lo que hay que imprimir varias pruebas.

   En el caso del libro objeto de este trabajo de investigación, hablamos del testeo de un proyecto editorial. La gestión de un proyecto editorial conlleva el desarrollo de una serie de procesos que comienzan en la presentación de una idea y culmina con la venta de la obra, bien sea un libro, una revista, una colección o cualquier otro documento impreso. No obstante, la gestión de proyectos editoriales va más allá del alcance del presente trabajo de investigación, razón por la que nos limitamos a incluirla como una fase más del proyecto de traducción y a ofrecer unas breves pinceladas al respecto. Podríamos afirmar, sin lugar a dudas, que

la traducción es una de las fases que forman parte de los proyectos de gestión editorial.

7. **Entrega final:** Una vez completadas todas las fases que hemos descrito con anterioridad, se realiza la entrega final al cliente en la forma acordada dentro del plazo establecido. Como hemos comentado con anterioridad, hay fases del trabajo que pertenecen a la editorial responsable del proyecto y a la agencia de traducción.

   En lo que se refiere al traductor, este debe tener en cuenta los pormenores del encargo y lo acordado con la agencia de traducción, ya que esta es su cliente final. En el caso del manual *CompTIA Security+,* la entrega del texto se realizó en documentos de Word independientes (uno por cada capítulo y las partes iniciales, es decir, prólogo, introducción, dedicatoria, agradecimientos, sobre el autor e índice). Las imágenes se entregaron en formato TIFF, junto con las capturas de pantalla.

8. **Seguimiento post-traducción:** Un trabajo no finaliza sin la conformidad del cliente. Unos días después de finalizar las traducciones, la agencia se pone en contacto con el cliente para conocer su satisfacción y para ofrecerle un servicio todavía mejor con su siguiente encargo.

   El traductor está en contacto con el jefe de proyecto y los revisores durante la realización del encargo, por lo que el seguimiento se realiza durante el proceso de traducción. De este modo, las correcciones y comentarios de los revisores se incluyen en los nuevos capítulos que se van traduciendo, lo que simplifica cada vez más el proceso de revisión.

Como podemos observar, se trata de un proceso complejo en el que intervienen muchos profesionales de distinto y tipo. Para que todo funcione, cada parte del equipo debe cumplir a tiempo su función. Por lo tanto, el traductor especializado debe disponer de las herramientas necesarias para realizar su trabajo en la fecha establecida. Podemos concluir que una de las herramientas más útiles que un traductor especializado puede emplear es la terminología para la creación de glosarios y sistemas de conceptos que no solo facilitan el entendimiento del texto de origen, sino que además agilizan el trabajo del traductor especializado que, en algunas ocasiones, tiene que cumplir plazos de entrega realmente ajustados.

3.2.1 Fases en el proceso de la traducción directa

En este epígrafe se describen las fases del proceso de traducción directa que lleva a cabo el traductor para realizar su trabajo. En general, realiza todas las fases de forma individual a excepción de la revisión. En el caso del manual que analizamos se llevaron a cabo tres tipos de revisiones:

1. **Realizada por el traductor antes de cada entrega:** En este tipo de revisión se realiza una comprobación de estilo y terminológica, el traductor pule su redacción y cualquier tipo de anomalía que encuentre en la segunda lectura del texto. Lo más recomendable es dejar pasar un tiempo mínimo para releer el texto con el fin de conseguir una redacción lo más fresca y ágil posible.

2. **Revisión estilística**: Realizada por un revisor de estilo. El corrector de estilo es un profesional de la edición y su tarea se enmarca en el control de calidad de la edición de textos. Por lo tanto, este tipo de revisión no solo se lleva a cabo en textos traducidos, sino en todo tipo de textos cuyo fin es ser publicados. En este sentido, el corrector de estilo interviene en el proceso de comunicación con el objetivo de evaluar si el emisor o autor del texto (en este caso, el traductor) ha conseguido expresar y redactar las ideas (del texto original) con la claridad necesaria para que el receptor elegido (profesionales del campo de la seguridad informática) pueda comprenderlas con facilidad o, si no es así, remediar los problemas.

3. **Revisión técnica**: Realizada por un revisor técnico experto en el tema del manual (seguridad informática). Cuando se trata de un texto especializado con fines didácticos, un experto en la materia debe revisar la terminología y el sistema de conceptos del texto meta. En este caso, resulta de gran utilidad y eficacia que el experto revise la base de datos terminológica con antelación a la finalización del proyecto para solventar posibles imprecisiones o errores terminológicos.

Como señalan Neunzig y Grauwinkel (2007), traducir no solo consiste en pasar de una lengua a otra; de ahí que propongan un modelo del proceso de traducción considerado como un acto de comunicación y transmisión de la información. También los investigadores del grupo PACTE de la Universidad Autónoma de Barcelona, que investiga la competencia traductora y analizan de forma sistemática el proceso de traducción de traductores profesionales y de

profesores de lengua en la traducción directa e inversa, han revisado el modelo del proceso de traducción. Respecto a las fases que intervienen en el proceso, han observado que la traducción directa sigue el modelo "clásico":

Análisis (LO) → Documentación (LO/LT) → Transferencia (LT) → Reformulación

Partimos de la hipótesis de que en la traducción directa la mayor competencia lingüística en la lengua de llegada se aprovecha en la revisión de la versión final de la traducción, en la cual el traductor resuelve los problemas que ha pospuesto en la fase de transferencia.

A continuación, se detalla una adaptación de cada una de las etapas del modelo de cinco fases de Neunzig y Grauwinkel (2007).

3.2.1.1 Fase 1: Aproximación al texto original con vistas a la traducción

Esta fase se dedica a la descodificación, recepción y análisis del texto original, así como a la detección de posibles problemas de traducción que pueda plantear el original. No solo nos podemos encontrar con problemas lingüísticos, también puede que tengamos que hacer frente a problemas técnicos, por ejemplo, localizar un software determinado para realizar las capturas de pantalla que se convertirán en las figuras del manual ya traducido. Otro caso de problema técnico que se debe solventar en esta fase es la adquisición de software para la traducción de imágenes, como el caso de las imágenes vectoriales.

Una dificultad específica de esta fase podría ser que el traductor no sea un especialista en el tema. De ahí, la importancia de que este sepa cómo sacar partido a las herramientas terminológicas para solventar esa carencia. En cualquier caso, la creación de una base de datos terminológica repercutirá de forma positiva en el proceso de traducción y en el resultado final.

3.2.1.2 Fase 2: Preparación del texto original de cara a la traducción

En esta fase el traductor prepara el texto original de cara a la traducción. En general, cuando se trabaja con agencias de traducción suelen proporcionar al traductor una guía de estilo, también conocida como especificaciones, en la que le indican las pautas a seguir para realizar la traducción. Algunas de las directrices se consignan en el siguiente cuadro resumen de las especificaciones que proporcionan al traductor las agencias de traducción.

Como cabe esperar, los requisitos varían mucho dependiendo del tipo de texto, de sus dimensiones, de la editorial de publicación, de la propia agencia de traducción y de cada proyecto. En este caso, resumimos algunas de las pautas generales que se deben seguir para la traducción de manuales extensos. Existen requisitos más concretos y específicos, pero solo pretendemos ofrecer una panorámica general lo más completa posible y acorde a nuestro proyecto.

Especificaciones generales de una agencia de traducción	
Procedimiento	* Protocolo de actuación al recibir el encargo de traducción. * Cómo presentar las entregas de los capítulos y sus figuras. * Importancia de las fechas de entrega semanales y finales.
Etiquetas de maquetación	* Varía de una empresa a otra. * Depende del tipo de texto. * **El traductor debe adaptarse a los requisitos de cada cliente.**

Recomendaciones generales	* **Traducción**
	  ○ Estrategias de traducción.
	  ○ Alerta sobre errores más comunes.
	  ○ Revisión.
	* **Redacción**
	  ○ Terminología (glosario): combinación de teclas, elementos de la interfaz de los programas, software, etc.
	* **Formato de texto**

Figuras y capturas de pantalla	* Capturas de pantalla e iconos. * Fotografías y dibujos. * Imágenes vectoriales. * Convertir formatos de archivos para obtener imágenes de mayor calidad. * Normativa sobre la entrega de imágenes.
Cómo hacer índices alfabéticos	* Solo se aplica en el caso de libros y manuales.
Normas para presentar CD-ROM	* Cómo hacer referencia a él dentro del manual. * Evaluar qué partes y archivos se traducen.
Configurar herramientas de trabajo	* Pantalla. * Procesador de textos. * Software para hacer capturas de pantalla. **OBJETIVO:** Homogeneizar el resultado final de los distintos traductores que colaboren con la agencia.

Tabla 4. Ejemplo de especificaciones generales de una agencia de traducción.

El objetivo de estas directrices no es otro que el de sistematizar la actividad de traducción y homogeneizar los resultados de los distintos traductores que colaboran con la agencia. Esta tabla solo ofrece una muestra general y resumida de algunas de las normas que deben seguir los traductores a la hora de realizar su trabajo. Por otro lado, cabe destacar que este profesional debe adaptarse a las pautas de trabajo de cada agencia o cliente y, por supuesto, al tipo de texto que vaya a traducir. Por ejemplo, esta tabla no es aplicable a documentos cortos o traducciones juradas (en este caso, el propio traductor marca las pautas de presentación de acuerdo con lo establecido en la ley).

Como podemos observar, esta tabla no hace mención alguna a la tarea terminológica y, por lo tanto, esta fase no se incluye ni en términos de tiempo ni de presupuesto. En este caso, es el traductor el que se ve obligado a organizar su tiempo para realizar la tarea terminológica sin remuneración alguna.

3.2.1.3 Fase 3: Preparación de la traducción

Una vez que el traductor conoce cuáles son las especificaciones que debe seguir, ha preparado sus herramientas de trabajo y se encuentra en disposición de los medios técnicos para realizar las capturas de pantalla, llega la fase dedicada a la documentación y la búsqueda de terminología.

El objetivo es optimizar el uso de las fuentes de información que el traductor tiene a su disposición: TICS, recursos tradicionales en formato papel e informatizadas.

Otra gran fuente a la que debe recurrir el traductor técnico de textos informáticos es el propio software sobre el que va a traducir, ya que allí encontrará la traducción de los programas y, con ella, los términos traducidos que se utilizan de forma real en el sector. Cabe también mencionar la importancia de ofrecer las rutas exactas que debe seguir el usuario a la hora de realizar un ejercicio o una tarea. A continuación, ofrecemos un ejemplo extraído del propio manual para ilustrar con mayor claridad a qué nos referimos.

- **Versión original:**

EXERCISE 12.1

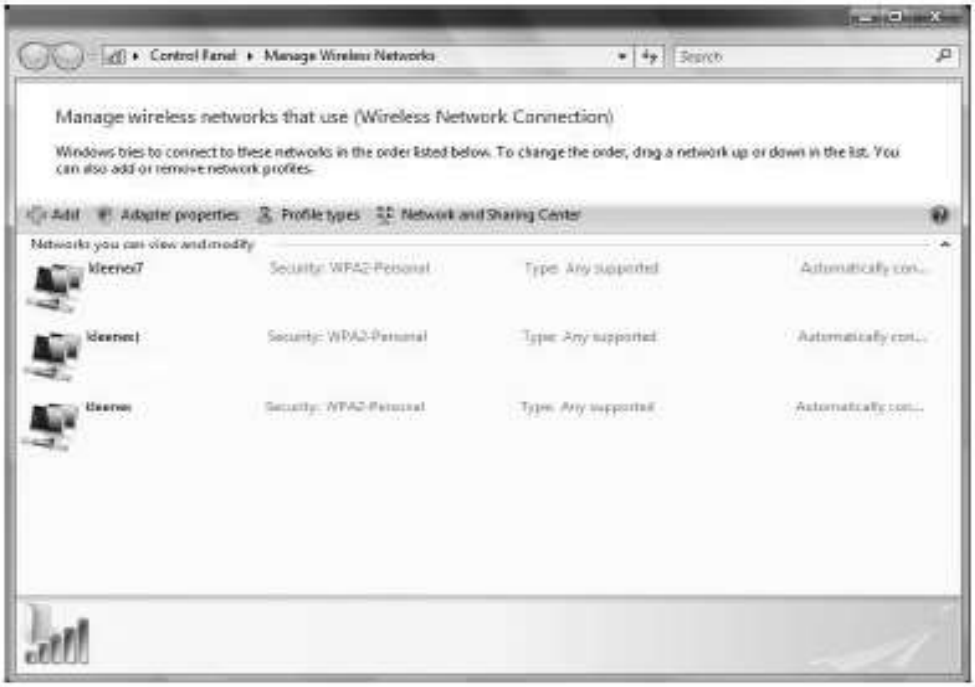
Change the Order of Preferred Networks

Most wireless clients are able to receive signals from, and connect to, more than one wireless network. If one wireless network is not available, the connection will often drop down to the next in this list, and thus it is important to have the wireless networks on the client in the order in which you want them to attempt connection. The following exercise will allow changes to this order:

1. On a Windows Vista client click the Windows button, type **Network and Sharing Center** into the search bar, and press Enter.

EXERCISE 12.1 *(continued)*

2. Choose Manage Wireless Networks.



3. Click any network that appears in the list, and drag it up or down to change the order of the preferred networks.
4. Exit out of Manage Wireless Networks.
5. Exit the Network and Sharing Center.

- **Versión traducida:**

Ejercicio 12.1. Cambiar el orden de las redes favoritas

La mayoría de clientes inalámbricos pueden recibir señales desde más de una red inalámbrica y conectarse a una de ellas. Si una red inalámbrica no está disponible, la conexión se realizará a través de la siguiente en la lista. Por esta razón, es importante que las redes inalámbricas estén en el orden que quiere para intentar la conexión. El siguiente ejercicio podrá modificar este orden:

1. En un cliente Windows Vista, haga clic en el botón **Windows**, escriba **Centro de redes y recursos compartidos** en el cuadro **Buscar** y pulse **Intro**.

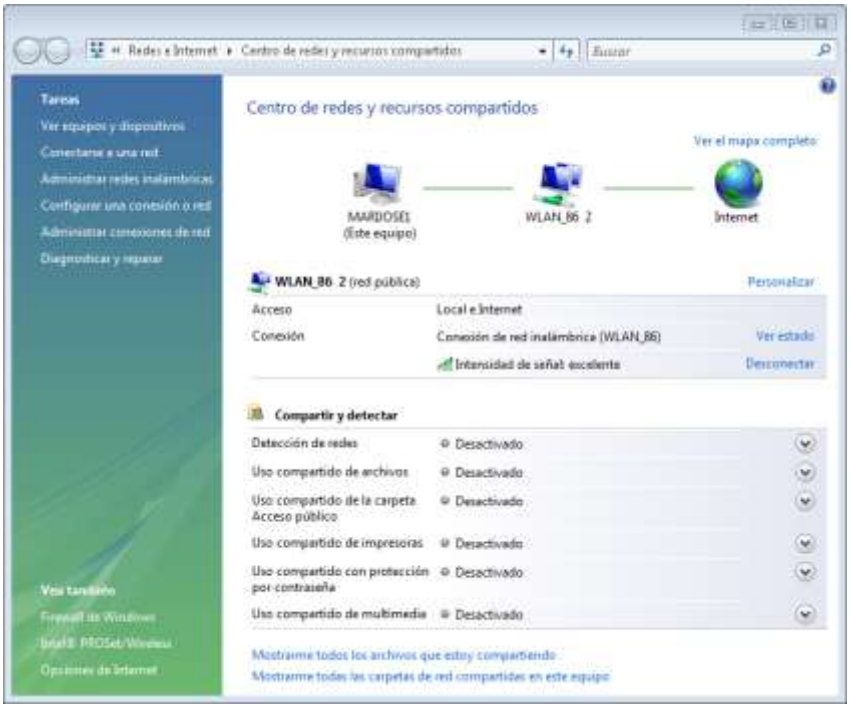


Figura 12.10. Centro de redes y recursos compartidos.

2. Seleccione **Administrar redes inalámbricas** (véase la figura 12.11).

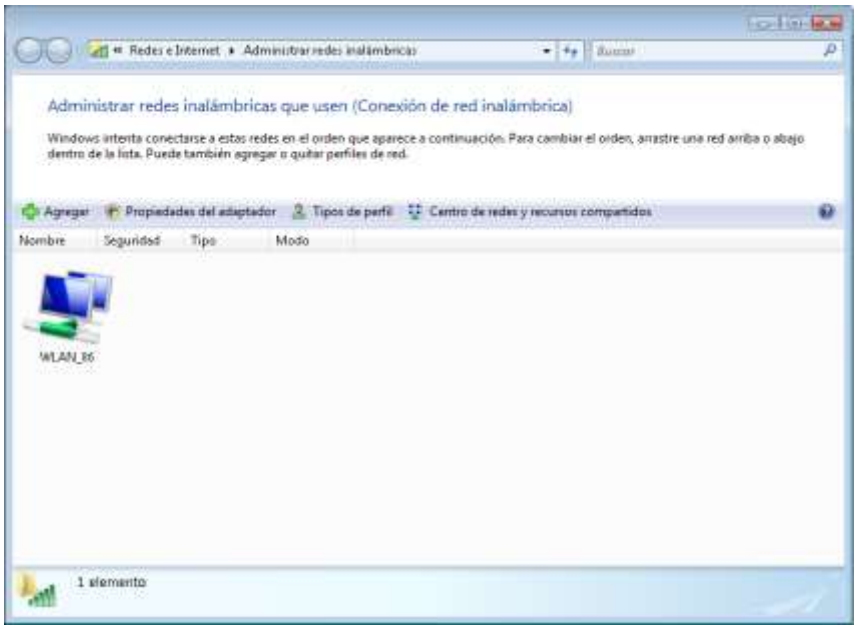


Figura 12.11. Administrar redes inalámbricas.

3. Haga clic en una de las redes que aparezcan en la lista y arrástrela hacia arriba o hacia abajo para cambiar el orden de las redes favoritas.
4. Salga de **Administrar redes inalámbricas**.
5. Salga de **Centro de redes y recursos compartidos**.

Como se puede observar, si no indicamos las rutas a seguir con total exactitud, podemos confundir al lector y dificultar enormemente la realización de ejercicio. Por esta razón, las interfaces de los programas y sistemas operativos serán una de las principales fuentes terminológicas del traductor técnico. El software es una fuente terminológica esencial para este proyecto y, como tal, determinará algunas estrategias de traducción para que prime la coherencia entre la interfaz del software y la terminología del texto meta.

3.2.1.4 Fase 4: Elaboración de la traducción

En esta fase se produce la traducción propiamente dicha, la transferencia lingüística que siempre debe adecuarse a las convenciones sintácticas formales, lingüísticas, estilísticas y culturales de la lengua de llegada. Además, el traductor debe tener en cuenta todas las especificaciones que hemos mencionado con anterioridad para conseguir un resultado que cumpla con las exigencias del cliente.

Es aquí donde el traductor vuelca la terminología y recurre a estrategias de traducción de diversa índole. En algunas ocasiones la terminológica resulta infructuosa, porque la equivalencia entre lenguas es parcial o nula. El traductor dispone de tres técnicas para solucionar el problema: préstamo, neologismo o paráfrasis. Cuando se decide por alguna de las dos primeras, idealmente debe consultar a un especialista en terminología, ya que la aparición de préstamos y neologismos no controlados supone un peligro para la armonización internacional de los términos, y al mismo tiempo favorece la excesiva proliferación de sinónimos.

A continuación, veremos algunos ejemplos de estas técnicas extraídas de la traducción propia realizada en agosto de 2011 de *CompTIA Security +.*

- **Préstamo:**

> *"Para que funcione, Evan tendría que haber accedido recientemente al sitio Web del banco y tener una cookie que todavía no haya expirado."*
>
> (pág. 6, archivo .doc 07)

Cookie: Archivo de texto simple almacenado en su máquina que contiene información sobre usted (y sus preferencias) y puede utilizarlo el servidor.

- **Neologismo:**

> *"En una LAN, los host pueden comunicarse entre sí utilizando las difusiones y no necesitan dispositivos de reenvío, como enrutadores."*
>
> (pág. 7 archivo .doc 05)

Enrutador: Un dispositivo que conecta redes separadas, que reenvía un paquete de una red a otra basándose solo en la dirección de red del protocolo que se está utilizando. Un enrutador determina la mejor ruta para los paquetes de datos desde el origen a su destino.

- **Paráfrasis:**

En general, se suele evitar la paráfrasis en la medida de lo posible y prima la utilización de las dos técnicas anteriores siempre que no haya una posible traducción del término en cuestión para otorgar al texto de mayor rigor científico y técnico, ya que la terminología es uno de los factores determinantes en la esencia del lenguaje técnico.

> *Risks Associated with Cloud Computing*
>
> Riesgos asociados a la computación en nube
>
> Hace poco tiempo que la popularidad del término computación en nube ha empezado a crecer, pero muy pocos se ponen de acuerdo a la hora de determinar qué significa en realidad.
>
> (pág. 4 archivo .doc 01)

3.2.1.5 Fase 5: Revisión

Esta fase varía dependiendo del contenido del libro. Puede llevarse a cabo una revisión técnica además de la estilística.

En este caso, estamos analizando un libro técnico de carácter formativo que se publicó como manual para preparar un examen de seguridad

informática. Por esta razón, como ya hemos señalado, se llevaron a cabo tres revisiones de distinto tipo:

1. Realizada por el traductor antes de cada entrega.
2. Revisión estilística: realizada por un revisor de estilo.
3. Revisión técnica: realizada por un revisor técnico experto en el tema del manual (seguridad informática).

En rasgos generales esta ha sido la metodología y las fases del trabajo que se han seguido para la traducción del manual *CompTIA Security +.* En el siguiente epígrafe nos centramos es describir el encargo y la hoja de proyecto para acotar el proceso de traducción de este manual en el tiempo y dotar al análisis de unos datos objetivos y reales, basados en la experiencia.

3.3 Terminología y traducción

Dada la fuerte presencia de la terminología en el proyecto de traducción que se analiza en este trabajo de investigación, este tercer apartado del capítulo 3 se centra en resumir brevemente la base teórica de esta disciplina para fundamentar su aplicación práctica en este proyecto. A continuación, se ofrece un recorrido por la historia y el desarrollo de la Terminología como ciencia, no sin antes destacar la estrecha relación existente entre terminología y traducción, así como la importancia que tienen las herramientas y la actividad terminológica para el traductor especializado.

Además de facilitar los procesos de comunicación entre distintos grupos de especialistas, la terminología se encarga de organizar el conocimiento. Por esta razón, también está relacionada con los procesos de documentación (en los que se ve involucrado el traductor en mayor o menor medida), así como con la lingüística computacional en la que se estudian los procedimientos de almacenamiento y recuperación de información. En este proyecto, sin embargo, nos centramos exclusivamente en la estrecha relación existente entre la terminología y la traducción especializada.

El conocimiento se materializa en términos, por lo que debe existir una correspondencia tanto de funcionalidad como de precisión en la traducción, lo cual permite que el texto alcance un sentido de naturalidad (IULA, 2005d). El traductor debe ser extremadamente riguroso al manejar el léxico con el

propósito de que los especialistas que lean el texto meta tengan la sensación de que lo ha redactado un colega. La única forma que tiene el traductor de conseguir este resultado es desarrollar algunas competencias que le permitan utilizar la terminología con precisión. Estas son las siguientes:

> **a. Competencia cognitiva:** Conocimiento del ámbito especializado que será objeto de trabajo.
>
> **b. Competencia lingüística:** Conocimiento sobre la lengua o las lenguas con las que se trabaja.
>
> **c. Competencia socio-funcional:** Características que debe tener un trabajo terminológico o la resolución puntual de un término para que resulte eficiente en relación a los fines que persigue y adecuado al texto o los destinatarios a los que se dirige.
>
> **d. Competencia metodológica:** La habilidad (…) para realizar un proceso de trabajo ordenado y sistemático, y presentar los datos de manera adecuada y eficiente para el trabajo que se realiza.
>
> (Cabré, 1999)

En este sentido, el traductor con formación en terminología es capaz de identificar el tipo de problema de carácter léxico que enfrenta, ponderar el grado de adecuación en el caso de la existencia de variantes para un mismo término, así como buscar soluciones adecuadas para esos problemas con el léxico especializado (IULA, 2005d). Dependiendo de su formación y del texto en cuestión, el traductor puede trabajar con la terminología a varios niveles.

Nadie dudaría que un traductor especializado necesita de la terminología, ya que una de las características principales de los textos especializados es la presencia de términos pertenecientes al sector en cuestión. A mayor cantidad de ellos, mayor grado de especialización. La comunicación especializada se distingue de forma básica por la especificidad del tema y de su perspectiva cognitiva. Esto influye en la terminología que lo compone. Las unidades terminológicas son las que condensan el conocimiento especializado. Por lo tanto, la densidad cognitiva es directamente proporcional a la cantidad de términos que contiene un texto y el grado de comprensión. En palabras de Cabré (2000:2):

> El traductor, mediador entre dos interlocutores hablantes de distintas lenguas, ejerce su función poniéndose en la piel del que emite el mensaje y asumiendo sus mismas competencias. Si no lo hace, difícilmente hará una buena traducción. Asumir las competencias de un productor de texto especializado comporta conocer la materia específica, controlar su contenido y manejar la terminología que lo expresa. Y para conseguir que

> el texto de traducción sea, en relación al original, literal en cuanto a contenido, gramatical en su expresión, adecuado en sus modalidades y ajustado estilísticamente, debe acercarse lo máximo posible a los usos léxicos que habría seleccionado el productor del texto si se hubiera expresado naturalmente en la lengua de la traducción. Debe servirse por tanto de los términos.

Para conseguir una traducción especializada de calidad es necesario recurrir de forma habitual a una terminología que se adecúe al grado de especialización del texto de trabajo y que sea real, es decir, que equivalga al uso efectivo que hacen de ella los especialistas. Por lo tanto, la terminología es importante para la traducción especializada y el traductor no puede dejar de utilizarla en sus textos (en distinto grado según el nivel de especialización del texto).

Sin embargo, el traductor no siempre tiene a su disposición de terminología de referencia, ni codificada en glosarios o bancos de datos lo bastante actualizada como para abarcar las necesidades de los temas actuales. Es por esta razón que se deben resolver estos problemas terminológicos que no resuelven las obras de consulta y, si lo hacen, la información no basta para poder realizar la selección de una unidad de equivalencia con total seguridad. De este modo, es el traductor el encargado de gestionar la terminología en el proceso de traducción para conseguir un texto de calidad.

En cualquier caso y con independencia del grado de especialización, el traductor necesitará tener conocimientos terminológicos: qué es, cómo se reconoce, en qué consiste un problema terminológico para la traducción, como se resuelve, qué pautas hay que seguir, etc.

Muchos de los glosarios disponibles no resuelven los problemas terminológicos del traductor por diversos motivos: no están actualizados, falta información o criterios de evaluación para su calidad y fiabilidad. Para que un glosario pueda resolver este tipo de problemas debe tener como punto de partida un análisis de las necesidades del traductor y adaptarse a las especificidades del texto en cuestión. Como cabe esperar, no se puede crear un glosario de calidad que cubra la necesidades terminológicas, que sea fácil de manejar y tenga una presentación adecuada sin tener unas nociones básicas de terminología.

En definitiva, traducción y terminología mantienen una relación muy estrecha que a veces resulta imposible de separar. En todo caso, el traductor

especializado no solo debe conocer el proceso de actividad de traducción, también es necesario que tenga formación terminológica, ya que utilizará esta disciplina en su trabajo diario y le será de extrema utilidad.

3.3.1 Historia y desarrollo de la Terminología

3.3.1.1 Orígenes y precursores de la Terminología

Aunque no se trata de una ciencia moderna, la terminología no se empieza a conocer y a desarrollar hasta a partir de los años 30 del siglo XX. Son los traductores de la Escuela de Toledo que organizó Alfonso X el Sabio (1221-1284) los primeros que apuntan sus dudas terminológicas en los márgenes de las traducciones. Leonardo da Vinci (1452-1519) es el pionero de la representación de conceptos en el Renacimiento (s. XV). De hecho, todavía no existen términos, ni objetos para los conceptos que él representa, como máquinas voladoras, puentes levadizos… La lengua se empieza a normalizar en el s. XVI. Surgen los primeros diccionarios que tienen una parte técnica de cierta importancia y aparecen los terminólogos lexicográficos. Un investigador que destaca en el desarrollo de la terminología es Andreas Versalius (1514-1564).

El auge de las ciencias que se produce durante el Despotismo Ilustrado (s. XVIII) propicia que los científicos empiecen a darse cuenta de la necesidad de reglas terminológicas que tengan en cuenta las relaciones entre conceptos (subordinación y coordinación). Científicos destacados en esta época son el químico Antoine-Laurent de Lavoisier (1743-1794), que manifiesta la importancia de la relación entre concepto y término para la comunicación en las ciencias, el médico y naturista Karl von Linné (1707-1778), quien contribuye con sus trabajos a la fijación de las denominaciones de los conceptos de las ciencias naturales, y Linné, creador de la nomenclatura binaria en botánica y zoología, gracias a la cual todos los seres vivos descubiertos tienen un nombre científico (*Fundamenta botánica*,1736). Antoine-Laurent de Lavoisier, Guyton de Morveau (1737-1816), Pierre E. Marcelin Berthelot (1827-1907) y Antoine Francois de Fourcroy (1755-1809) idean una nomenclatura química unificada y clara tomando como base las raíces etimológicas de las sustancias químicas. Por su parte, el economista Johann Beckmann (1739-1811) sostiene que para elaborar una terminología sistemática en los ámbitos citados hay que

deshacerse de numerosos sinónimos, eliminar términos que representan distintos conceptos e introducir nuevas denominaciones.

A partir del siglo XIX, con la revolución industrial, se intenta resolver el descontento de los científicos ante la insuficiencia de material comunicativo. Así, botánicos, zoólogos y químicos expresan, en sus respectivos coloquios internacionales de 1867, 1889 y 1892, la necesidad de disponer de reglas de formación de términos para cada disciplina. Para el siglo XIX, influenciado por la internacionalización del progreso de la ciencia, surge la necesidad de establecer reglas sistemáticas que faciliten los procesos de creación de los términos en cada disciplina. De los trabajos en terminología realizados durante este periodo destaca la *Nomenclatura Anatómica Clásica*.

Llegado el siglo XX, la tarea de la terminología se enfoca hacia la denominación de los conceptos así como a la armonización de nuevas denominaciones. Esto se debe al acelerado progreso de las ramas técnicas y el desarrollo tecnológico. Es durante este siglo cuando surgen las primeras escuelas de terminología. En 1904, se crea la Primera Asociación Internacional en Missouri: Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés), cuyo propósito fue normalizar el vocabulario electrotécnico producido. Posteriormente, en Alemania, Eugen Wüster funda la Escuela de Viena en 1931, y años más tarde propone la Teoría General de la Terminología. Para la década de los años cincuenta, los lingüistas se interesan por crear una teoría que dé cuenta de los principios que rigen a las lenguas.

No obstante, el verdadero desarrollo de la terminología tiene lugar a partir de los años treinta. Poco antes de la Primera Guerra Mundial surgen en Europa una serie de Escuelas Superiores de Estudios Mercantiles en las que se enseñan los Lenguajes Especializados. Esta corriente, llamada Wirtschafts-Linguistik, predica un tipo de lingüística que sintetiza los conocimientos profesionales de las diferentes ciencias unidos a estudios lingüísticos. En la Wirtschafts-Linguistik surgen varias corrientes, de entre las cuales destacan dos:

- Una muy tradicional y teórica basada en la filología.

- Otra que se apoya en la lingüística aplicada y en la Escuela de Praga.

Podemos concluir que en el siglo XX aparece la Terminología Moderna. Resumimos su evolución por medio del siguiente cuadro (Cabré, 1993):

Evolución de la Terminología Moderna	
Orígenes (1930 – 1960)	Sistematicidad de los métodos de trabajo terminológico (Wüster, Lotte). Tendencias: ➢ Percepción generalizada del carácter sistemático de las terminologías. ➢ Principio de aplicación de técnicas lexicográficas y terminográficas que se desprenden del carácter sistemático de las terminologías. ➢ Reconocimiento de la terminología en el campo internacional.
Estructuración (1960 – 1975)	En ella tienen lugar tres hechos relevantes: ➢ Desarrollo de los sistemas informáticos y las técnicas documentales. ➢ Creación de Bancos de Datos. ➢ Creación de la Organización Internacional de la Terminología.
Eclosión (1975 – 1985)	➢ La informática se pone al servicio de la terminología. Época del ordenador personal. ➢ Planificación lingüística (modernización de la lengua): URSS, Israel. ➢ Cambio en las condiciones del trabajo terminológico y el tratamiento de los datos. ➢ Avance en terminografía.
Horizontes (desde 1985)	➢ Instrumentos y recursos de trabajo (aportes de la informática). ➢ Nuevos mercados de las industrias del lenguaje. ➢ Cooperación internacional. ➢ Consolidación del modelo de la terminología ligada a la planificación de la lengua. ➢ Investigación y formación en terminología.

Tabla 5. Evolución de la Terminología Moderna.

Para Rondeau (1984), la terminología es un fenómeno socio-económico/lingüístico. La gran eclosión que vive hoy en día se explica por los cambios acaecidos a principios del siglo XX y que exponemos a continuación:

1) **El avance de la ciencia y la técnica:** El gran desarrollo de la ciencia y la técnica provoca la aparición de una gran cantidad de conceptos y campos conceptuales nuevos, que requieren nuevas denominaciones.

2) **El espectacular desarrollo de la tecnología:** Surgen nuevas disciplinas (aeronáutica, informática, telecomunicaciones, etc.) que generan una avalancha de nuevos conceptos, con sus correspondientes designaciones, que tienen un equivalente inmediato en otras lenguas.

3) **Desarrollo de los medios de comunicación:** Por ello, muchos términos científico-técnicos se incorporan poco a poco al léxico general y empiezan a ser utilizados de forma activa.

4) **Desarrollo de las relaciones políticas internacionales:** Tras la Segunda Guerra Mundial (1939-1945) se crean organismos internacionales tales como la ONU, la OTAN, etc., cuya meta es establecer normas internacionales. Estas normas, postuladas en un primer idioma (en general, el inglés), no cuentan, a menudo, con un equivalente en otras lenguas. Surge, pues, la necesidad de normalizar conceptos y términos en sectores tales como el derecho internacional y la política.

5) **Desarrollo del comercio internacional:** Los intercambios comerciales internacionales también favorecen el desarrollo de nuevas terminologías y la aparición de la Wirtschaftslinguistik.

6) **Impulso de las multinacionales:** Para que no existan barreras a la hora de vender sus productos, las multinacionales generan y normalizan su terminología en su lengua y en otras lenguas extranjeras.

7) **La aceptación de la normalización por el público en general:** Se manifiesta, cada vez más, una actitud positiva hacia la normalización en todas las actividades cotidianas (medios de transporte, objetos de uso corriente, costumbres, etc.).

8) **La intervención de los gobiernos en materia lingüística:** Provoca la inclusión de la terminología en los planes de normalización y planificación de las lenguas y la creación de organismos oficiales para gestionarla.

Auger (1988) establece tres grandes tendencias en terminología que atienden a las finalidades de sus diversos enfoques:

TENDENCIA	CARACTERÍSTICAS
Lingüístico-terminológica	Está representada por tres escuelas: ➢ **Viena:** Basada en los trabajos de Wüster, adopta los principios de la Teoría General de la Terminología. Es la única escuela que desarrolla un corpus sistemático de principios y fundamentos que constituyen la base de toda la terminología teórica y práctica moderna. ➢ **Praga:** Basada en las teorías de Saussure (1987). Se ha ocupado de la investigación del lenguaje normalizado en todos los niveles, pero sobre todo en el tecnológico. ➢ **Moscú:** Basada en los trabajos de Wüster, presenta dos vertientes: - Una perfecta continuación entre la teoría y la práctica. - Tratamiento lingüístico de los problemas terminológicos.
Traduccionalista	La terminología ha estado unida a las facultades de traducción. Por ello se constituye el banco de datos terminológicos. Representa también el elemento más importante que ha impulsado la creación de bancos de datos terminológicos (ej.: TERMIUM, del gobierno canadiense; EURODICAUTOM, de la CEE; BTQ, del gobierno de Québec).
Normalización	Surge en los años 70 como consecuencia de la tendencia anterior. Da lugar a la Escuela de Québec que se funda con la finalidad de conseguir un estatuto normal para el francés. Se dedica a la investigación de sus propias terminologías, a su normalización, difusión e implantación.

Tabla 6. Grandes tendencias en terminología.

No obstante, podemos encontrar otras clasificaciones como la de Laurén y Picht (1993: 493-536), que establecen cinco escuelas o corrientes: la Corriente Canadiense, la Escuela de Praga, el Círculo Nórdico, la Escuela Soviética y la Escuela de Viena.

Por otra parte, los Países Nórdicos (Círculo Nórdico) adoptan una postura pragmática: reconocen y trasladan claramente a la práctica la necesidad de colaborar con otras disciplinas. Para ellos la terminología es una disciplina de unión.

Por último, la Escuela Soviética, cuyos máximos representantes son Lotte y Caplygin, subraya la conexión que existe entre las disciplinas lingüísticas en igual medida que con las no lingüísticas. No obstante, esta escuela aproxima sus posiciones a las de la Escuela de Viena.

A modo de conclusión, cabe destacar que el objetivo fundamental de la terminología, en el que coinciden todas las escuelas y corrientes, es el de asegurar y mejorar la comunicación especializada. Esto deja claro, sin lugar a dudas, por qué esta disciplina es tan importante para el profesional de la traducción especializada.

3.3.1.2 La Teoría Comunicativa de la Terminología

Durante la segunda mitad del siglo XX se han producido innumerables cambios a todos los niveles (social, económico, tecnológico) que han propiciado la reconsideración de la terminología, ya que los escenarios no sólo están limitados a la mera normalización. Surge así la necesidad de abarcar la complejidad en términos de representación y comunicación para adaptarse a la nueva realidad.

Este nuevo contexto social y lingüístico ha aumentado de forma drástica la demanda de servicios de comunicación multilingües (por ejemplo, en la Unión Europea, Organización de las Naciones Unidas, UNESCO…). Por otra parte, el impresionante desarrollo de las tecnologías ha llevado a la aparición de nuevas herramientas profesionales de gran valor (programas de traducción asistida, herramientas de extracción terminológica, software para la digitalización de archivos, reconocimiento de texto…). Como cabe esperar, todo esto ha hecho que se incremente el número de profesionales dedicados a la traducción y la interpretación, la gestión lingüística o el procesamiento automático de las lenguas.

De este modo, durante la década de los 90, surge una alternativa a los principios clásicos de la terminología de manos de Cabré (1999) que plantea

una serie de reflexiones que sentaría las bases de la Teoría Comunicativa de la Terminología (TCT).

Como alternativa a los postulados de la terminología clásica, Cabré (1999) recoge una serie de reflexiones que serían el fundamento de la Teoría Comunicativa de la Terminología (TCT). En palabras de Cabré (1999: 122-4), estas ideas se podrían resumir en los siguientes puntos[20]:

1. **La terminología es una materia interdisciplinar** que integra aportaciones de la teoría del conocimiento, relativas a los tipos de conceptualización de la realidad y a la relación de los conceptos entre sí y con sus posibles denominaciones.

2. El objeto de estudio son las **unidades terminológicas** que forman parte del lenguaje natural. Los términos no son unidades autónomas que forman un léxico especializado diferenciado, sino que se describen como unidades denominativo-conceptuales, dotadas de capacidad de referencia, que pueden ejercer funciones distintas e integradas en el discurso. **El carácter de término se activa en función de su uso en un contexto y situación determinados.**

3. Los términos son unidades de forma y contenido en las que el contenido es simultáneo a la forma. **Un contenido puede ser expresado con mayor o menor rigor por otras denominaciones del sistema lingüístico,** que constituyen nuevas unidades lingüísticas de contenido especializado relacionadas semánticamente con la primera, o por denominaciones de otros sistemas simbólicos, que conforman unidades no lingüísticas de contenido especializado.

4. Los conceptos de un mismo ámbito especializado mantienen entre sí relaciones de diferente tipo. El conjunto de estas relaciones entre los conceptos constituye la estructura

[20] Véase:
M. T. Cabré: "La Teoría Comunicativa de la Terminología, una aproximación lingüística a los términos", *Revue française de linguistique appliquée*, 2/2009 (Vol. XIV), p. 9-15. 2009.
URL : <http://www.cairn.info/revue-francaise-de-linguistique-appliquee-2009-2-page-9.htm>
[Fecha de consulta: 20 de octubre, 2016]

conceptual de la materia. **Así, el valor de un término se establece por el lugar que ocupa en la estructuración conceptual.**

5. El objetivo de la terminología teórica es el de describir formal, semántica y funcionalmente las unidades que pueden adquirir valor terminológico, dar cuenta de cómo lo activan y explicar sus relaciones con otros tipos de signos del mismo o distinto sistema. **La finalidad aplicada de la recopilación y análisis de las unidades de valor terminológico usadas en un ámbito es muy diversa y permite muchas aplicaciones.**

Hacemos especial hincapié en estas ideas de la Teoría Comunicativa de la Terminología por su especial relación con el presente trabajo de investigación, así como también por su actualidad y adaptación a la nueva realidad del mundo de las tecnologías aplicadas. Una de las muchas aplicaciones que permite la recopilación y el análisis del valor terminológico es la recopilación de términos especializados de un campo del saber para su uso en la práctica de la traducción profesional. Esto nos permite acotar los términos a la estructuración conceptual de la materia. Por otra parte, los sistemas de conceptos[21] que aparecen en el proyecto terminológico de este trabajo de investigación son un claro ejemplo de relaciones entre los conceptos que llevan a una estructuración conceptual de la materia en cuestión, en este caso, la seguridad informática.

3.3.1.2 Historia y desarrollo de la Terminología en España

La importancia de la terminología en España es muy reciente. No obstante, ya a mediados del s. XIX la Real Academia de Ciencias creó un *Diccionario de términos técnicos.* Para nuestra sorpresa, en el diario del político y escritor Manuel Azaña (1880-1940), ya se comenta que en 1926 imparten una asignatura de terminología en bachillerato.

Tras algunos acercamientos a esta disciplina, en 1970 el Consejo Superior de Investigaciones Científicas (CSIC), en colaboración con otras instituciones, decide cooperar en un proyecto para establecer de un fondo

[21] Véase: Proyecto terminológico. Capítulo 6.

terminológico de lenguas neolatinas. A pesar de su interés, tras varias reuniones, la iniciativa decae y el proyecto no sigue adelante.

En 1977, con motivo de unas Jornadas Internacionales de Investigación Humanística, el CSIC crea un centro de terminología científica y técnica para el castellano, HISPANOTERM. En 1978 inicia un Programa para la Coordinación de la Lengua Científica Española, gracias al cual se celebra el Primer Seminario de Terminología en España impulsado por Manuel Criado de Val. En este seminario participan Felber y Pich. Sin embargo, no tuvo mucho éxito. Asimismo, en 1981y 1985, el CSIC aprueba unos proyectos de investigación en terminología. Pero el paso fundamental se produce cuando en 1985 instituye Termesp. Desde entonces, este grupo trabaja en terminología y representa internacionalmente la terminología española en lengua castellana.

Del mismo modo, la Asociación Española de Normalización y Racionalización (AENOR), que se fundó en 1986, trabaja con la terminología. En 1991, tras el Seminario sobre programa de los cursos de Terminología en la Licenciatura de Traducción e Interpretación en España (Gallardo y Sánchez, 1992), se idea un programa para esta materia que se empieza a impartir, desde 1993, como asignatura troncal (Ministerio de Educación y Ciencia, BOE 234/91), en las Facultades de Traducción e Interpretación de España. Con ello, esta ciencia experimenta un nuevo impulso.

Por último, representantes de la terminología española en distintos ámbitos (empresas privadas, Facultades de Traducción e Interpretación, centros oficiales que se interesan por la terminología, etc.), convocados por el CSIC, constituyen en diciembre de 1997 la Asociación Española de Terminología (AET),que significa un nuevo paso en la expansión de esta ciencia en España.

No podemos dejar de mencionar el trabajo realizado por el Institut Universitari de Lingüística Aplicada (IULA), fundado por María Teresa Cabré Castellví, Catedrática de terminología y lingüística de la Universitat Pompeu Fabra, desde 1994. Dentro del IULA se creó el grupo de investigación IULATERM[22], un grupo de investigación consolidado y con gran reconocimiento

[22] Véase: IULATERM (Lèxic, terminologia, discurs especialitzat i enginyeria lingüística)
URL: < http://www.iula.upf.edu/iulaterm/>
[Fecha de consulta: 20 de diciembre, 2016]

en el ámbito de la lingüística aplicada al léxico (léxico, terminología, neología, discurso especializado y tecnologías asociadas).

3.4. Lingüística de corpus: Herramientas de extracción terminológica

En este epígrafe definiremos qué es la lingüística de corpus y presentaremos algunas herramientas de extracción terminológica que podemos utilizar en nuestra labor terminológica y traductológica. También incluiremos ejemplos que permitan ilustrar la teoría a un nivel más práctico y concreto. Por último, nos centraremos en las aplicaciones de la lingüística de corpus a la traducción y, de forma más específica, a la traducción especializada.

3.4.1 Lingüística de corpus

La lingüística de corpus es una ciencia que se ha desarrollado gracias a la innovación tecnológica. Sinclair, en su libro *Corpus, Concordance, Collocation* (1991: 1), resume la evolución de la lingüística de corpus del siguiente modo:

> Thirty years ago when this research started it was considered impossible to process texts of several million words in length. Twenty years ago it was considered marginally possible but lunatic. Ten years ago it was considered quite possible but still lunatic. Today is very popular.

A su vez, define el corpus como "A collection of naturally occurring language text, chosen to characterize a state or variety of a language" (1991: 171). La lingüística de corpus es, pues, la rama de la lingüística que utiliza corpus para analizar la lengua y determinar sus características, verificar teorías lingüísticas o ensayar aplicaciones de la ingeniería lingüística.

La lingüística del corpus se define como una metodología empírica que se dedica a la enseñanza y al estudio de la lengua. Parte del uso de muestras reales del uso de la lengua que se erigen en un conjunto de datos reales; estos se conocen como "corpus" en un sentido general. Una extensa tradición de estudios lingüísticos avala esta metodología; sin embargo, es innegable que el uso de ordenadores como sistema de organización de estos datos ha supuesto

el gran auge de la lingüística de corpus en un sentido moderno del término "corpus".

En cuanto a los antecedentes de la lingüística de corpus, podemos destacar que, antes de la llegada del ordenador, hasta el siglo XIX los trabajos lingüísticos que se basaban en el corpus se caracterizaban por conjuntos de datos de textos escritos, cuya finalidad era el estudio de lenguas muertas como el latín y el sánscrito. Se erigía así como una necesidad, ya que este era el único acercamiento posible a estas lenguas que ya no se hablaban.

Esta metodología de trabajo que parte de la recogida de muchos datos escritos (lo que conocemos como corpus) fue la dominante hasta el último tercio del siglo XIX y hasta mediados del siglo XX para documentar el proceso de adquisición del lenguaje mediante la transcripción de interacciones infantiles, establecer convenciones de índole ortográfica, recopilar listas terminológicas para la enseñanza de idiomas, llevar a cabo estudios comparativos de las lenguas y desarrollar gramáticas descriptivas.

Sin embargo, las bases de la lingüística del corpus no se sentaron hasta la primera mitad del siglo XX, momento en el que se estableció como metodología empírica y basada en la observación de datos. El término como tal no se acuñó hasta principios de los 80, dado que, según esta teoría, se creía que el corpus proporcionaba por sí solo los datos necesarios para una descripción exhaustiva para el estudio de las lenguas. Las características del corpus estructuralista son las siguientes: el conjunto de datos lo forman muestras orales o transcripciones en papel, su finalidad es el estudio de lenguas vivas que no se hayan documentado por escrito previamente (lenguas amerindias) y satisface la necesidad de recoger datos orales era la única forma de acceder al conocimiento de esas lenguas.

3.4.1.1 Chomsky y Abercrombie: críticos de la lingüística del corpus inicial

Durante los años 60 y 70, con la irrupción de la figura de Chomsky, se produjo una ruptura con los primeros trabajos en lingüística del corpus de los estructuralistas americanos y, de este modo, se dio paso a la lingüística de corpus actual. Con Chomsky se impone el racionalismo como filosofía de fondo que debe guiar las investigaciones relacionadas con el lenguaje. Esta fue una época de duras críticas a la metodología empírica.

A raíz de estas críticas, la metodología basada en corpus (empirismo) experimentó un desprestigio general en pos de una ortodoxia enfocada en una aproximación que se basaba en las intuiciones del lingüista (racionalismo). No obstante, se siguieron elaborando corpus en campos concretos en los que el uso de muestras reales de la lengua era totalmente necesario. Por ejemplo, fonética (requiere datos, ningún tipo de juicio de valor), adquisición de lenguas (los niños no han desarrollado su capacidad metalingüística) y lingüística histórica (en casos en los que no se podía recurrir a los hablantes).

Chomsky hizo varias críticas a los córpora que fundamentalmente partían de su rechazo al paradigma estructuralista, oponiéndose de forma radical al uso de cualquier metodología descriptiva en la teoría lingüística: “[...] linguistic theory is mentalistic since it is concerned with discovering the mental reality underlying actual behaviour” (1965: 4). Por tanto, a Chomsky le interesa estudiar las reglas subyacentes que determinan la interpretación de un número indeterminado de oraciones en una lengua determinada. En este sentido, solo está interesado en un hablante-oyente ideal, que sabe su lengua perfectamente, y aplica su conocimiento lingüístico en el uso real (*performance*), sin verse afectado por ninguna condición "gramaticalmente irrelevante", tales como las limitaciones de la memoria o las pequeñas distracciones o errores (1965: 24): “[...] a grammar is descriptively adequate to the extent that it correctly describes the intrinsic competence of the idealised native speaker.”

Recordemos la conocida distinción propuesta por Chomsky entre *competence*, el conocimiento interiorizado de una lengua, y *performance*, la evidencia externa de la competencia lingüística:

> [...] Like most facts of interest and importance [...] information about the speaker-hearer’s competence [...] is neither presented for direct observation nor extractable from data by inductive procedures of any unknown sort. (1965: 18)

La consecuencia de estas críticas fue la irrupción de una nueva ortodoxia en los estudios lingüísticos, un acercamiento que se basa en las intuiciones del lingüista (racionalismo).

Además de las críticas teóricas de Chomsky, también había problemas prácticos en la primera lingüística de corpus. Abercrombie (1965) resumió el acercamiento basado en corpus como "pseudo-técnicas", ya que el procesamiento de datos era lento, propenso al error y caro, al tener que ser

realizado por personas. Estas críticas prácticas no carecían de razón. La primera lingüística de corpus necesitaba de habilidades de procesamiento de datos que no estaban disponibles en esa época. El hecho de que el trabajo lo tuvieran que llevar a cabo personas encarecía el proceso y reducía la fiabilidad de los análisis. Como cabe esperar, fue la llegada del ordenador la que dio un nuevo impulso a la lingüística basada en el corpus.

La compilación del primer corpus informatizado organizado sistemáticamente se abordó en Estados Unidos. A partir de ese momento, los corpus electrónicos se convirtieron en recursos imprescindibles para distintos fines relacionados con la investigación lingüística.

Entre las características más destacadas de los corpus de estas décadas se encuentra las que detallamos a continuación. En primer lugar, el establecimiento del vínculo entre los corpus y los ordenadores. Los datos tenían un carácter representativo, ya que la mayoría de los proyectos de elaboración de corpus se concebían pensando en su posterior informatización. No obstante, ya durante la década de los 50, A. Juilland estableció los conceptos de marco de la muestra, representatividad y equilibrio, básicos en el concepto actual de corpus (McEnery, 2003: 452). Por otra parte, predominaban los corpus de textos escritos, aunque con notables excepciones, ya que había una tendencia a desfavorecer los datos orales por las dificultades técnicas y de transcripción. En cuanto al tamaño, giraba en torno al millón de palabras.

En este período, encontramos algunos corpus destacados:

- ***Survey of English Usage Corpus* (*SEU*)[23]:** R. Quirk (University College, Londres) estableció las bases para la elaboración de este corpus en 1951. Su recopilación empezó en 1961 con el fin de erigirse como una descripción sistemática del inglés británico hablado y escrito (1955-1985). El encargado de completar este proyecto fue S. Greenbaum. Fue clave para la futura lingüística de corpus. En la actualidad, está informatizado, aunque no se diseñó como corpus electrónico.

[23] URL: Survey of English Usage Corpus <http://www.ucl.ac.uk/english-usage> [Fecha de consulta: 14 de diciembre, 2016]

- ***Brown University Corpus of American English* (*Brown Corpus*)[24]:** Realizado en EE.UU. por N. Francis y H. Kucera. Se trata de un corpus de 1 millón de palabras extraídas de 500 muestras de unas 2000 palabras recopiladas de publicaciones de Estados Unidos de 1961. Su fin es mostrar el inglés americano escrito. Además, es el primer corpus ideado para ser informatizado.

- ***Lancaster-Oslo/Bergen Corpus* (*LOB*)[25]:** Realizado por G. Leech (Universidad de Lancaster), S. Johansson (Universidad de Oslo) y el Norwegian Computing Centre for the Humanities en Bergen. Se trata de un corpus de 1 millón de palabras que recopila de inglés británico escrito en 1961.

Si bien es cierto que se trata de corpus muy pequeños en comparación con algunas colecciones a gran escala de la actualidad, se siguen utilizando en el ámbito de la investigación por la gran utilidad de contar con una estructura planificada y representativa.

3.4.1.2 Resurgir de la lingüística del corpus

La lingüística del corpus se mantuvo como disciplina minoritaria durante los 60 y 70. Su resurgir no se produjo hasta la década de los 80 gracias a autores como G. Leech, que rebatieron las críticas de índole práctica y teórica formuladas contra la primera lingüística de corpus.

Para Leech (1992), la lingüística de corpus no es un campo ni un área de estudio. Por el contrario, se trata de un terreno determinado por el especial interés en los corpus basados en metodologías muy diferentes y que son fruto de la incorporación de los avances tecnológicos, así como de ciertas categorías paradigmáticas. Sinclair (1991) y Simpson y Swales (2001) argumentan que la lingüística es una técnica o una tecnología, cuyo fundamento es el corpus mismo y cuya clave está en la construcción adecuada de un corpus

[24] URL: Brown University Corpus of American English
<http://clwww.essex.ac.uk/w3c/corpus_ling/content/corpora/list/private/brown/brown.html> y
<http://icame.uib.no/brown/bcm.html> (manual).
[Fecha de consulta: 14 de diciembre, 2016]

[25] URL: Lancaster-Oslo/Bergen Corpus
< http://khnt.hit.uib.no/icame/manuals/lob/INDEX.HTM> (manual) y
<http://khnt.hit.uib.no/icame/manuals/lobman/INDEX.HTM> (anotaciones).
[Fecha de consulta: 14 de diciembre, 2016]

representativo de forma planificada. De este modo, los resultados generados a partir del corpus podrán ofrecer una relación directa con la constitución de la base de datos.

Algunos de los argumentos que aporta Leech (1992:259) a favor de los corpus son los siguientes:

- Como metodología científica el corpus proporciona varias ventajas porque está ligado a la verificación, descartando así la aparición de ejemplos inventados por los lingüistas de forma interesada.

- La mayoría de enunciados de un corpus son gramaticales, por lo que los corpus reflejan la competencia. Los trabajos de Labov (1969) mostraron el alto porcentaje de secuencias gramaticales en un corpus.

- Los corpus son un recurso de incalculable valor para recopilar datos cuantitativos. Los datos relativos a la frecuencia de uso serán representativos de la lengua en su totalidad, siempre que el corpus esté bien diseñado.

- Los ordenadores tienen la capacidad de procesar gran cantidad de datos a un coste reducido, de forma mucho más rápida que las personas y sin cometer errores.

En la década de los 80 y gracias a las nuevas ventajas y posibilidades que ofrecían los ordenadores, los corpus electrónicos se convirtieron en una herramienta imprescindible para estudiar el lenguaje, probar hipótesis lingüísticas y construir sistemas de procesamiento del lenguaje natural. Solo en ese momento se generaliza el término, sobre todo a partir de 1984, año en que J. Aarts y W. Meijs editaron el volumen titulado *Corpus Linguistics I: Recent Developments in the Use of Computer Corpora*, y se empieza a hablar de lingüística de corpus en el sentido actual del término.

3.4.2 Herramientas de extracción terminológica

La extracción terminológica se ha realizado tradicionalmente de forma manual, es decir, se procedía a la lectura del corpus y a la extracción de los

términos que se consideraban relevantes. Aunque en la actualidad nos cueste creerlo, no hace tanto tiempo de esto. Una vez seleccionados los términos, estos se trasladaban a bases de datos terminológicas o glosarios que se destinaban a facilitar la labor del traductor.

No obstante, en la actualidad, debido a los avances en el campo de la tecnología, esta labor se ha simplificado de manera muy significativa, puesto que existen numerosos programas TAO, cuyo objetivo consiste en extraer los términos de forma automática. Más adelante, describiremos de forma breve algunos programas TAO que tienen como objetivo extraer términos de forma automática

Las herramientas de extracción terminológica hacen que sea posible identificar y extraer términos potenciales de los corpus textuales analizados. En el caso de este trabajo de investigación, se ha llevado a cabo una extracción de términos usando como corpus textual los cinco capítulos analizados. Como cabe esperar, la finalidad de estas herramientas es crear contenido para las bases terminológicas. Se podría decir que son el punto de partida para que el traductor o el equipo de traducción realicen los análisis y las evaluaciones pertinentes para decidir qué términos se incluirán de forma definitiva en la base de datos terminológica.

En el presente trabajo de investigación, a la hora de seleccionar los términos que pasarán a formar parte de la base de datos terminológica, la intuición profesional se une a las posibilidades que ofrecen las herramientas de extracción terminológica. Es decir, empleamos las ventajas que ofrecen las nuevas tecnologías y aplicamos los conocimientos teóricos que hemos ido adquiriendo; sin embargo, también damos cabida a la intuición profesional que nos lleva a detectar términos de forma rápida y eficaz. Por supuesto, esta parcela concedida a la intuición se revisa posteriormente, de modo que las comprobaciones terminológicas puedan confirmar que realmente se trata de un término especializado en el campo de la seguridad informática y que la selección del mismo no se debe a un desconocimiento por parte del traductor.

En nuestra opinión, la combinación de estas herramientas y conocimientos junto a la intuición profesional es el método más idóneo y eficaz para realizar la extracción terminológica y seleccionar los términos especializados que formarán parte de nuestra base de datos terminológica adaptada de forma definitiva.

Las herramientas de extracción terminológica resultan especialmente útiles y ventajosas en el campo de la gestión de la información y el conocimiento. Por otra parte, la gestión de la terminología es una práctica recomendada para evitar trasladar conceptos confusos al mercado. La posibilidad de extraer de forma automática los términos de un corpus textual también facilita y favorece la creación de glosarios específicos. Extraer palabras clave para realizar un análisis definitivo con posterioridad posibilita el establecimiento de unidades de indexación. Esto abre un enorme campo de posibilidades al traductor especializado.

A pesar de la multitud de ventajas que ofrecen, las herramientas de extracción terminológica automáticas presentan algunos problemas relacionados con la naturaleza lingüística de los términos. También encontramos problemas a la hora de detectar y distinguir entre términos y no términos, con independencia de que sean simples o compuestos. Es ahí donde entra en juego la labor del traductor especializado o del terminólogo.

Para llegar a unos resultados de calidad que nos permitan establecer la extracción terminológica de forma satisfactoria hemos de establecer ciertos parámetros y un diseño conceptual (que utilizaremos con posterioridad para elaborar los sistemas de conceptos de nuestro proyecto terminológico) que nos permita solucionar estos problemas. También es posible establecer el uso de algoritmos que definan nuestras estrategias de extracción terminológica.

Por otra parte, debido a los problemas que se encuentran al integrar las herramientas de extracción terminológicas en sistemas de traducción asistida, nuestro planteamiento ha sido el siguiente:

1. Extracción terminológica con el uso de herramientas de extracción terminológica (AntCont).

2. Revisión y análisis de los resultados.

3. Selección definitiva de los términos.

4. Creación de las fichas terminológicas y el glosario bilingüe.

5. Volcado de estas fichas en una base de datos terminológica (Multiterm 2014).

6. Revisión y análisis de los resultados. Comprobación del correcto funcionamiento de la base de datos creada en Multiterm y su adecuado funcionamiento en combinación con Trados 2014.

7. Integración de la base de datos terminológica en un programa de traducción asistida.

8. Creación y optimización del proyecto de traducción en Trados 2014 para que se adapte a las especificaciones de nuestro trabajo de investigación.

9. Creación de una memoria de traducción de forma simultánea al proceso de traducción integrada en el proyecto de traducción.

10. Análisis de los resultados.

3.4.2.1 Algunos ejemplos de herramientas de extracción terminológica

Como ya hemos comentado, las herramientas de extracción terminológica siguen unas pautas que establecemos nosotros mismos. Por ejemplo, podemos determinar si queremos ignorar abreviaturas o cuantificar qué mínimo de términos forma una expresión. En base a estas directrices, el programa selecciona los términos pertinentes para dar paso a la posterior evaluación del traductor.

Algunos extractores de terminología ofrecen la posibilidad de integrarlos en herramientas TAO. No obstante, muchos de ellos trabajan de forma autónoma. Entre los más conocidos destacan:

- ***+Extract*:** Esta herramienta está incluida en las *+Tools* de Wordfast, que es un motor de Memoria de Traducción diseñado para Microsoft Word en PC y Mac. A pesar de que Wordfast es básicamente una herramienta para traductores, se integra fácilmente en los procesos de agencias de traducción y grandes empresas. Es un software libre que permite optimizar la gestión y el tratamiento de la información.

- ***Text API*:** Es una herramienta en línea de AlchemyAPI de la compañía IBM que ofrece análisis textual mediante el procesamiento del lenguaje natural.

Además, facilita la extracción de las palabras de ficheros de diversa naturaleza con el fin de seleccionar los términos relevantes para el proyecto en cuestión.

- ***Term Extraction*:** Software gratuito y libre de FiveFilters. Surge como alternativa a *Yahoo's Terms Extraction*. Nos ofrece la posibilidad de trabajar en varios formatos. Por ejemplo, HTML, JSON, XML y el texto simple.

A continuación ofrecemos una pequeña muestra de una extracción terminológica realizada on-line en la interfaz de AlchemyLanguage. En este caso, los resultados son satisfactorios, ya que el término *control de acceso* es un término específico del ámbito de la seguridad informática. Si lo introducimos en nuestra base de datos terminológica, evitamos que este término se traduzca de varias formas diferentes en nuestro texto o que se emplee una forma sinónima del mismo, como por ejemplo, *control de entrada, control de llegada, inspección de acceso, examen de llegada o vigilancia de acercamiento.* Estos ejemplos pueden ser más o menos apropiados, pero ponen de manifiesto la riqueza léxica del español. Además, esto nos permite hacernos una idea de la calidad de los resultados que podemos obtener implementado las herramientas de extracción terminológica.

Figura 6. Introduccción del texto para realizar el análisis.

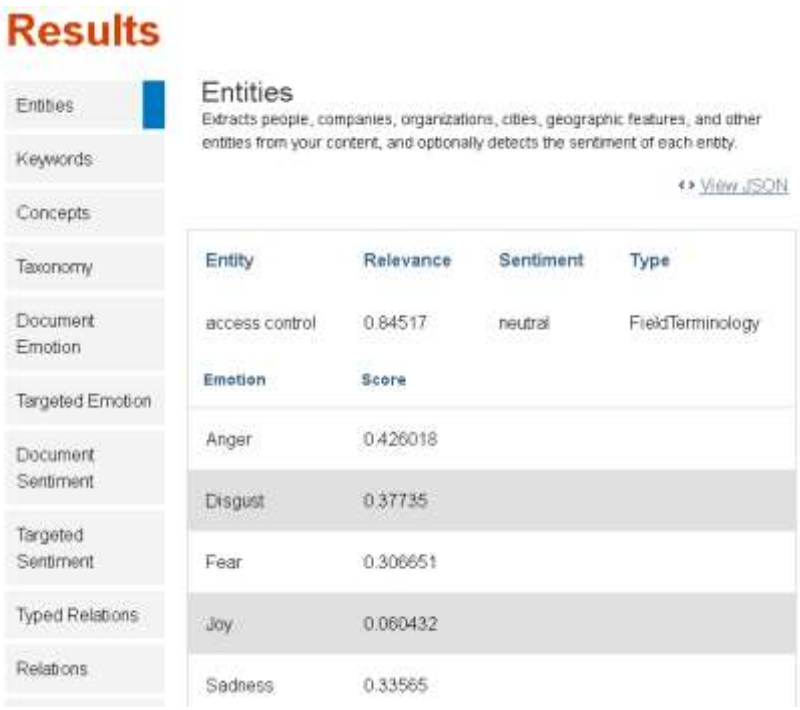


Figura 7. Resultados de una extracción terminológica.

3.4.2.2 AntConc

AntConc es un software libre para el análisis de corpus textuales. Esta herramienta nos ofrece un paquete de software independiente que nos permite el análisis lingüístico de textos en un PDF o un documento de Word. Está disponible para Windows, Mac OS y Linux.

> El análisis de corpus es una forma de análisis de texto que le permite hacer comparaciones entre los objetos de texto a gran escala (llamada "lectura distante"). Lo que permite ver cosas que no vemos como lectores habituales. Si se dispone de una colección de documentos, es posible que se desee encontrar patrones de uso gramatical, o frases que se repiten con frecuencia en el corpus. Así como encontrar frases estadísticamente probables y / o improbables para un autor o tipo de texto en particular, determinados tipos de estructuras gramaticales o una gran cantidad de ejemplos de un concepto en particular en un número amplio de documentos en su contexto. Análisis Corpus es especialmente útil para triangulación de textos resultados de otros métodos digitales."
>
> Blog de Traducción e Interpretación de la biblioteca de la USAL

A continuación presentamos una pequeña muestra de extracción terminológica realizada con AntCont.[26] Hemos utilizado el mismo término que en el ejemplo anterior: *access control*. Este programa nos permite, además, comprobar la frecuencia de aparición del término elegido.

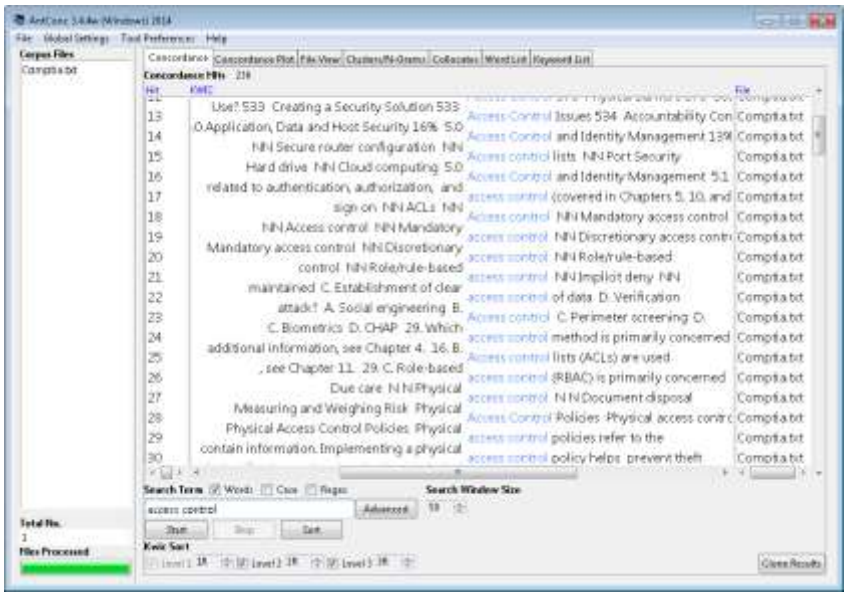


Figura 8. Extracción terminológica en AntConc.

Figura 9. Comprobación del número de apariciones de un término en AntConc.

[26] El creador de AntCont es el profesor Laurence Anthony de la Facultad de Ciencias e Ingeniería de la Universidad de Waseda, Japón. Además, es el antiguo director de Center for English Language Education (CELESE) y el coordinador del programa de inglés técnico de CELESE. Véase:

L. Anthony: *"Introducing corpora and corpus tools into the technical writing classroom through Data-Driven Learning (DDL)".* En J. Flowerdew and T. Costley (eds.) *Discipline Specific Writing*. Abingdon, UK: Routledge, 2016.

Como podemos observar, esta herramienta ofrece multitud de posibilidades para la gestión terminológica de nuestros proyectos, siendo especialmente útil en el caso de trabajos de gran envergadura, ya que nos permite volcar estos resultados en bases de datos y glosarios que no solo nos facilitan en trabajo como traductores, sino que, además, nos llevan a conseguir mejores resultados y mayor coherencia. Todo esto facilitará la lectura de nuestras traducciones y evitará la creación de traducciones dobles que generen confusión en el lector. Como cabe imaginar, esto es aún más importante si cabe en el caso de los textos técnicos como el que nos ocupa, en los que una confusión puede generar multitud de problemas en el lector.

Figura 10. Comparaciones de frecuencia con vista a la discriminación de términos.

Establecer comparaciones de frecuencia nos permite decidir si una palabra en cuestión es o no un término, así como crear gráficos de frecuencia. No hay duda de que a los traductores nos merece la pena incorporar estas herramientas de extracción terminológica por multitud de factores, por ejemplo, para la creación de bases de datos terminológicas adaptadas a un proyecto, la sistematización del trabajo, la optimización de la tarea documental y la mayor calidad de las traducciones.

3.4.3 Aplicaciones de la lingüística de corpus a la traducción

Para establecer una serie de aplicaciones de la lingüística de corpus a la traducción[27], partimos de una definición técnica de lingüística del corpus:

> A collection of machine-readable authentic texts (including transcripts of spoken data) which is sampled to be representative of a particular language or language variety and which may be annotated with various forms of linguistic information.
>
> (Francis, 1992: 17)

Existe una gran variedad de corpus. Por ejemplo, podemos distinguirlos en base al número de lenguas que incluyen, encontrando así corpus monolingües o bilingües, y en algunos casos también corpus multilingües. Por otra parte, también podemos establecer como parámetro de clasificación si se trata de textos originales o textos traducidos.

Si nos centramos en la relación entre Lingüística de corpus y Traducción encontramos dos opciones: corpus para estudiar distintas estrategias de traducción con fines investigadores y corpus que sirvan como recurso para la traducción. En nuestro caso, nos centramos en los corpus destinados a la creación de una base de datos terminológica adaptada a un proyecto en concreto.

¿Por qué crear una base de datos terminológica adaptada a un proyecto en concreto?

1. La creación de una base de datos terminológica adaptada al proyecto de traducción (en este caso de seguridad informática) nos permite el uso de las tecnologías de traducción más avanzadas y novedosas, con las consiguientes ventajas que esto comporta.

2. El término se traduce una vez, pero se utiliza muchas veces. Esto agiliza la labor de traducción. El traductor solo tiene que realizar una vez la búsqueda documental. El resultado final de la traducción es más coherente. Por lo tanto, la gestión terminológica nos permite ofrecer traducciones de mayor calidad.

3. La creación de una base terminológica a partir de un corpus incrementa el conocimiento en todos los dominios. En este caso, esta labor

[27] Véanse a este respecto: Francis, 1992; Atkins, Clear & Ostler, 1992; McEnery, Xiao & Tono 2006.

terminológica otorga al traductor un conocimiento especializado del campo de la seguridad informática.

4. La implementación de herramientas de gestión terminológicas en proyectos de traducción proporciona una sistematización del trabajo que permite profundizar en la búsqueda documental.

5. La tecnología avanza a pasos agigantados y cambia constantemente, por lo que en muchas ocasiones los diccionarios no pueden ayudarnos, ya que la información que ofrecen no está actualizada.

6. Algunos de los corpus de referencia de grandes dimensiones incluyen el mayor número textos posibles de todo tipo de especialidades del conocimiento, como, por ejemplo, el *Corpus de Referencia del Español Actual* (CREA) de la Real Academia Española o *The Bank of English* de Cobuild y la Universidad de Birmingham. Otro ejemplo a nivel europeo sería el IATE (*Inter-Active Terminology for Europe*), la base de datos de referencia de la UE, que puede utilizar todo el mundo y engloba todas las bases de datos terminológicas creadas en el marco de la Comisión Europea.

Figura 11. Búsqueda terminológica en IATE.

Como observamos en esta imagen, hay varias opciones posibles para traducir *access control* en función del ámbito de especialidad. Acceder a una base de datos terminológica adaptada a nuestro proyecto nos permite optimizar tiempo y búsquedas, ya que al volcar nuestras fichas terminológicas en una herramienta de traducción asistida, aparecerá exclusivamente la traducción que seleccionamos al principio durante el proceso de gestión terminológica.

Ofrecemos a continuación un esquema resumen de las ventajas de la creación de una base de datos terminológica para un proyecto concreto:

CREACIÓN DE UNA BASE DE DATOS TERMINOLÓGICA EN-ES: *COMPUTER SECURITY*

- Futuros usos.
- Se puede volcar en diferentes herramientas de traducción asistida para su posterior uso.
- En el caso de equipo de traducción: favorece la coherencia y la cohesión del texto. Permite y facilita el trabajo en equipo. Simplifica la labor de traducción, ya que todos los traductores utilizarán la misma base de datos terminológica.
- Rentabiliza el trabajo.
- Actualización de futuras ediciones del manual.
- Coherencia terminológica.
- Coherencia a la hora de redactar el texto: uso de estructuras similares.
- Sistematización del trabajo: los términos solo se buscan una vez.
- Se evitan las duplicidades de términos o que se adopten distintas estrategias de traducción para un mismo término.
- CONCLUSIÓN: Repercute en la calidad final de texto meta.

Figura 12. Ventajas de la creación de una base de datos terminológica EN-ES para el proyecto *Comptia Security+.*

Al margen de todas estas ventajas, hoy en día los traductores especializados recurrimos al gran portal que ofrece Internet para iniciar la fase de documentación, ya que es ahí donde podemos encontrar la información más actualizada de forma inmediata. Sin embargo, la información relacionada con el ámbito de la seguridad informática (y con la informática en general) cambia y se actualiza a gran velocidad; de hecho, cuando empezamos a traducir ciertos proyectos ni siquiera encontramos esta información en la red, ya que no existe nada publicado en español al respecto. En estos casos, el traductor

especializado introduce nuevos términos en el lenguaje de destino. No obstante, una vez que localizamos un texto, escaneamos la información que necesitamos, por ejemplo, un término o una expresión lingüística determinada. En muchas ocasiones, recurrimos a foros de profesionales del sector, porque no hay nada escrito en español sobre estos temas tan actuales y nuestro proyecto será la primera publicación en español sobre el tema. Hacer uso de la lingüística del corpus durante esta fase documental permite al traductor optimizar su tiempo y sus recursos gracias a estas herramientas de extracción terminológica que hemos comentado con anterioridad.

La compilación de textos paralelos con el fin de documentarse en un breve período de tiempo lleva a la creación de los corpus *ad hoc* (denominación acuñada por Aston (1999)). De este modo, elaboramos un pequeño diccionario especializado para nuestro proyecto que parte de ejemplos reales utilizados por los propios expertos en la materia.

Por último, no hemos de olvidar cuestiones como la fiabilidad y la relevancia de los textos y términos seleccionados. Zanettin (2002: 240) advierte que podemos encontrar varios problemas relacionados con el uso de los documentos extraídos de Internet:

> The first concerns procedures for assessing relevance and reliability: Information is dispersed in the WWW through vast quantities of documents, and it is thus crucial for the translator to retrieve this information in the most efficient and effective way. The second relates to strategies and techniques for searching electronic texts: Search engines provide access points to Internet documents either through lists generated by full text searches or by pre-selected lists organized by topic, and are thus catalogues rather than corpora.

Como hemos señalado antes, nuestra propuesta es aplicar la lingüística de corpus para crear herramientas y recursos que se incorporen a la práctica profesional del traductor especializado. El objetivo de este trabajo de investigación no es otro que poner de manifiesto algunas de las posibilidades que esta ofrece.

3.5 Gestión terminológica para la traducción

La selección y la definición, así como la coherencia y el correcto uso de los términos especializados son requisitos fundamentales para una traducción de calidad. Por esta razón, los traductores hemos de entender la terminología del texto original y hemos de seleccionar y utilizar los equivalentes adecuados en la lengua de destino. En proyectos de traducción de gran envergadura en los que intervienen varios traductores, la fase de investigación terminológica y la especificación de la terminología del idioma de destino es especialmente importante y debe empezar antes de que se inicie el proyecto de traducción principal. Por consiguiente, el traductor debe involucrarse en el trabajo terminológico y abordar los sistemas de gestión terminológica. Además, el traductor debe ser consciente de sus necesidades específicas y de cómo va a aplicar las herramientas de gestión terminológica a sus proyectos. Como cabe imaginar, cada proyecto tendrá sus propias necesidades terminológicas.

Otro factor digno de tener en cuenta es que, en el mercado de la traducción, la mayoría de los proyectos se encargan a agencias de traducción que trabajan con profesionales independientes (traductores, revisores, maquetadores), con el objeto de que realicen las tareas lingüísticas de traducción y revisión. El número de empleados que trabajan a nivel interno suele ser muy reducido y no suelen tener formación terminológica. Por otra parte, lo general suele ser que los traductores internos se centren en la revisión de los textos y, en algún caso, en la terminología.

Cuando la agencia de traducción no proporciona un glosario para un proyecto de gran envergadura surge la pregunta de cómo reaccionará el traductor. ¿Va a limitarse a traducir el texto usando los glosarios existentes que pueda encontrar por sí mismo sin sacar partido del tiempo que invierte documentándose? ¿Creará su propio glosario? Y si hay varios traductores implicados en el proceso, ¿utilizarán todos el mismo glosario?, ¿compartirán sus propios glosarios?, ¿se prestarán a ello?

Si la agencia no paga al traductor por la realización de estas tareas, habrá quien se cuestione si le merece la pena al traductor crear sus propios glosarios. Nuestra opinión es un sí rotundo. No solo por todos los motivos que hemos mencionado con anterioridad, sino también para futuros proyectos similares o para llevar a cabo actualizaciones del mismo manual que se editen con posterioridad. No obstante, clientes y agencias de traducción deben ser

conscientes de este problema que se acentúa cuando se trabaja con equipos de traducción a los que no se les proporciona un glosario para homogeneizar la terminología. Para nosotros, es de suma importancia tener en cuenta todas estas cuestiones a la hora de abordar un proyecto de traducción, ya que nos lleva a mejores resultados y sistematiza la tarea de traducción.

Entender las implicaciones de la terminología y su papel clave en el proceso de traducción también implica aceptar que, para implementarla de forma óptima, hay que dedicar tiempo y dinero. Por esta razón, es crucial que todas las partes involucradas en un proyecto de traducción sean conscientes de unas cuestiones básicas:

1. La base de datos terminológica y, por lo tanto, el glosario son herramientas a largo plazo.
2. Es un trabajo inicial que se puede amortizar, ya que se puede utilizar para futuros proyectos relacionados con el tema.
3. Utilizar una terminología cohesionada y sistemática ahorra tiempo de revisión.
4. La base de datos terminológica garantiza que los manuales y la documentación corporativa siempre serán precisos y coherentes, es decir, que los términos siempre se traducirán del mismo modo.
5. Se optimiza el proceso de redacción, traducción y corrección de la documentación corporativa, con significativos ahorros en costes.
6. A nivel de empresa, se refuerza la imagen e identidad corporativa frente a terceros gracias a una comunicación coherente en estilo y vocabulario.
7. A nivel de profesional independiente, se agiliza el trabajo y los tiempos de entrega. Además, ofrece rigurosidad y uniformidad a nuestros proyectos.
8. En el caso de que introduzcamos nuevos términos en español, mantendremos unas estrategias de traducción coherentes y consistentes en todos los proyectos que realicemos sobre esta temática y no introduciremos dobles opciones de traducción.

Por último, podemos destacar que las fases que comprenden un proyecto de Gestión Terminológica son las que aparecen en el siguiente

diagrama:

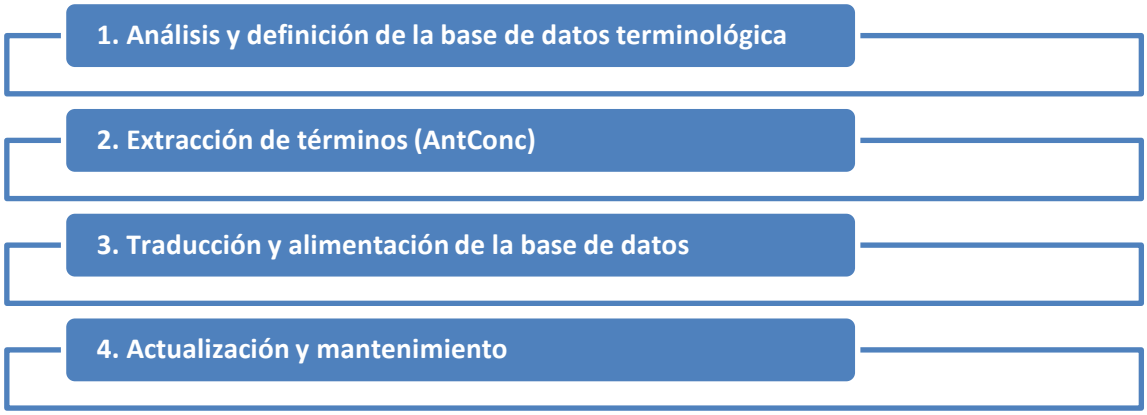


Figura 13. Fases de gestión terminológica.

Una vez elaborada la base de datos de seguridad informática ya solo hay que mantenerla y actualizarla cuando sea necesario, por lo que el proceso se simplifica aún más de cara a futuros proyectos del mismo ámbito de especialidad.

Podemos concluir siempre es un valor añadido el hecho de que un traductor especializado preste servicios de terminología y gestión terminológica de forma exhaustiva, así como también personalizada y adaptada a los distintos proyectos que realice, lo que redundará en una mayor uniformización lingüística y coherencia conceptual. Esto permite presentar toda la información de forma organizada y estructurada en forma de base de datos.

4. ENCARGO, HOJA DE PROYECTO, TRADUCCIÓN Y FIGURAS

En este capítulo repasamos el encargo, la hoja de proyecto concreta que fue proporcionada por la agencia de traducción y mencionamos de forma breve las consideraciones específicas del encargo. Esta información nos sirve como documento real de la práctica profesional, ya que gracias a él podemos analizar la planificación, el tiempo dedicado a la traducción y los factores a los que presta atención una agencia de traducción del mundo real.

Se trata de un capítulo breve, que solo se limita a reflejar la información de la que se partió para poner en marcha este proyecto de traducción de forma clara y objetiva.

Con estos datos, podemos observar qué importancia se le da a la fase terminológica o a la fase técnica de un proyecto de traducción y cómo es el propio traductor el que debe abordar estas cuestiones en términos de tiempo y sin remuneración. Por lo tanto, se pone de manifiesto cómo esto implica un gran esfuerzo personal adicional, que lamentablemente la mayoría de agencias no tienen en cuenta a día de hoy.

Así pues, el debate está servido. ¿Deben las agencias de traducción tener en cuenta estos factores? ¿Es el traductor el que debe encargarse de todo ello de forma aislada? ¿Sería favorable para ambas partes abordar estas cuestiones de forma conjunta? Como punto de partida, este capítulo solo pretende mostrar de forma objetiva cómo es una de proyecto real y cuáles son los aspectos que tiene en cuenta.

4.2 Hoja de proyecto

Como ya hemos mencionado, el encargo consiste en la traducción de *CompTIA Security* + de inglés a español, un manual sobre seguridad informática que se publica en español con el objetivo de preparar un examen para técnicos en la materia.

Una vez confirmada la asignación del encargo, el jefe de proyecto envía al traductor[28] una hoja de proyecto similar a la que aparece a continuación en la que se estipula la fecha de inicio y la fecha final del encargo, así como las unidades por entrega semanal y las características específicas del encargo.

<table>
<tr><td colspan="2">Páginas: 650</td><td colspan="2">Fecha de inicio: 10 de junio de 2011</td></tr>
<tr><td colspan="2">Fecha estimada:
7 de agosto de 2011</td><td colspan="2">Unidades por entrega:
81 páginas (semanales)</td></tr>
<tr><td colspan="2">Idioma origen: Inglés</td><td colspan="2">Idioma destino: Español</td></tr>
<tr><td>1º Entrega 12-jun-11
Material Portada-00</td><td>2º Entrega 19-jun-11
Material Caps 01-02</td><td>3º Entrega 26-jun-11
Material Caps 03-04</td><td>4º Entrega 3-jul-11
Material Caps 05-06</td></tr>
<tr><td>5º Entrega 10-jul-11
Material Caps 07-08</td><td>6º Entrega 17-jul-11
Material Caps 09-10</td><td>7º Entrega 24-jul-11
Material Caps 11-12</td><td>8º Entrega 31-jul-11
Material Caps 13-14</td></tr>
<tr><td>9º Entrega 7-ago-11
Material Caps 15-Fin</td><td>----------</td><td>----------</td><td>----------</td></tr>
<tr><td colspan="4">Características específicas del encargo:
* Seguir guías de estilo de la empresa.
* Cambiar unidades monetarias a euros siempre que no rompa el sentido del texto.
* Dado que es un libro de formación, se va a revisar técnicamente.</td></tr>
</table>

Tabla 7. Hoja de proyecto del encargo.

[28] La persona encargada de traducir la totalidad del proyecto es la misma persona que ha realizado el presente trabajo de investigación.

4.2 Consideraciones específicas del encargo

Como podemos observar, no hay un plazo establecido para la fase terminológica y técnica del proyecto. Tampoco se ofrece un glosario que satisfaga las necesidades terminológicas del proyecto. Por lo tanto, esta labor recae sobre el traductor especializado.

Dado que se trata de un libro de formación, se realizó una revisión técnica durante la traducción del manual. La retroalimentación entre los revisores (de estilo y técnico) y el traductor fue constante durante todo el proceso. Como consideraciones específicas del encargo habría que tener en cuenta la terminología técnica y la naturaleza didáctica del texto.

Una dificultad es la necesidad de agilizar lo más posible el proceso de documentación, ya que debido a las ajustadas fechas de entrega no siempre se cuenta con un plazo para llevar a cabo un proceso exhaustivo de documentación. Este proceso de documentación sirve simultáneamente para tres propósitos: adquirir conocimientos sobre el campo temático, lograr el dominio de la terminología propia del mismo y obtener información sobre las normas de funcionamiento del género. Los tres factores hacen necesario que el traductor se documente antes de realizar su trabajo; habrá de hacerlo de una forma amplia y suficiente, en función de sus conocimientos y de la dificultad del texto, e integrando los tres objetivos cuando sea posible, con el fin de rentabilizar el proceso.

Por otra parte, el traductor es el encargado de realizar la traducción de las figuras y capturas de pantalla que aparecen en el manual. Para ello, este debe contar con todas las herramientas necesarias:

- **Software para hacer captura de pantalla:** (también llamada pantallazo, o *screenshot*) Imagen tomada por un ordenador para capturar los elementos que aparecen en el monitor u otro dispositivo de salida visual. En general, es una imagen digital tomada por el sistema operativo o aplicaciones que se están ejecutando en el ordenador.

  Las capturas de pantalla se suelen usar para ilustrar y explicar un programa, un problema particular que un usuario pueda tener o, de

manera más general, cuando la salida de la pantalla se debe mostrar a otros o ser archivada.

La manera más habitual de realizar una captura de pantalla es pulsando la tecla Imprimir Pantalla (a veces llamada Print Screen Imp Pant o SysRq PrtSc) situada en la parte superior derecha del teclado. Dependiendo del sistema operativo o entorno de escritorio, el proceso de la captura puede variar.

- **Software para la edición de imágenes:** La edición digital de imágenes se ocupa de la edición en ordenador de imágenes digitales, comúnmente un gráfico rasterizado[29], en la mayoría de los casos fotos o documentos escaneados. Estas imágenes se modifican para optimizarlas, manipularlas, retocarlas, etc., con el fin de alcanzar la meta deseada. En este caso, el objetivo es traducir el texto que contengan obteniendo una calidad adecuada para la maquetación e impresión del documento.

- **Herramientas de traducción asistida:** Son programas informáticos específicos; por ejemplo, los que crean y organizan memorias de traducción y los editores de recursos interactivos de software de tipo textual, también llamados herramientas de localización.[30]

Una vez que el traductor dispone de la hoja de proyecto, el material original (incluyendo las figuras para su edición) y todo el software que va a necesitar para la realización del proyecto, puede empezar a traducir y realizar las capturas de pantalla en el idioma de destino. En la mayoría de ocasiones es el propio traductor el que ha de encargarse de adquirir todo el software que va a necesitar para el proyecto; como es lógico, esto requiere tiempo, algo que no se refleja en el cronograma de la hoja de proyecto.

[29] Rasterización de capas de texto: Algunos comandos y herramientas, como los efectos de filtro y las herramientas de pintura, no están disponibles para capas de texto. Para poder aplicar el comando o utilizar la herramienta, antes se debe rasterizar el texto. Rasterizar convierte la capa de texto en una capa normal y hace que su contenido sea imposible de editar como texto.
Léase al respecto la Ayuda de Adobe: URL:
<http://help.adobe.com/es_ES/photoshop/cs/using/WSfd1234e1c4b69f30ea53e41001031ab64-75c8a.html.> [Fecha de consulta: 13 de diciembre, 2016]

[30] Dada la extensa variedad de herramientas disponibles en el mercado tanto de pago como gratuitas, este trabajo de investigación no profundiza más en este aspecto. Algunos ejemplos son: OmegaT, Trados, Wordfast, etc. No obstante, destacamos y valoramos enormemente su utilidad. Puede encontrarse una aplicación gratuita en la URL:
<http://www.omegat.org/es/omegat.html>. [Fecha de consulta: 13 de diciembre, 2016]

5. MEMORIA DE TRADUCCIÓN

En este capítulo nos centramos en la memoria de traducción, entendida como un repaso del proceso de traducción, así como de sus dificultades, y no a la acepción de corpus lingüístico paralelo de texto original y texto traducido. En ella analizamos las principales dificultades del proceso de traducción, la fase de la búsqueda documental, así como algunos problemas terminológicos y documentales que encontramos a lo largo del proceso.

5.1 Principales dificultades del proceso de traducción

Uno de los primeros retos consistió en el logro del equilibrio necesario en la traducción de un texto de carácter híbrido. Como comentamos al inicio de este trabajo, este texto en particular reúne las características de los textos técnicos y divulgativos. Por este motivo, se habían de tener en cuenta las peculiaridades de ambas tipologías textuales. Recordemos muy brevemente las características de ambos tipos de textos:

- **Textos de divulgación**: se trata de aquellos textos que difunden y promocionan determinados productos científicos y técnicos, así como el uso de los mismos. Son ejemplos de este tipo los textos informativos, los textos publicitarios, los manuales y guías de usuario, etc.

- **Textos técnicos**: son aquellos que tratan temas relacionados con las matemáticas, nuevas tecnologías, ingenierías, informática, arquitectura, etc. Ejemplos de esta tipología pueden ser los artículos o manuales universitarios que versan sobre estas materias, informes de arquitectura, etc.

- **Textos tecno-científicos o híbridos**: constituyen un tipo textual que integra, con diferentes grados de especialización, documentos relacionados con ciencias híbridas, es decir: bioestadística, microbiología, biología molecular, etc.

  Sin embargo, en el caso del presente trabajo de investigación nos referimos a otro tipo de naturaleza híbrida. En el manual analizado, está claro que predomina la temática técnica, en especial, el texto se centra en el ámbito

> de la seguridad informática, por lo que su naturaleza es claramente técnica. Su carácter híbrido proviene de la funcionalidad del mismo y no de su ámbito del saber, ya que nos encontramos ante un texto técnico con una funcionalidad claramente didáctica y divulgativa. Por lo tanto, aquí se entrelaza la univocidad del lenguaje técnico con la claridad de los textos didácticos. Si bien es cierto que este manual se dirige a un público muy concreto (profesionales de la seguridad informática) y no generalizado.

Una segunda dificultad consistió en agilizar al máximo el proceso de documentación, ya que debido a las ajustadas fechas de entrega no siempre se cuenta con un plazo para llevar a cabo un proceso exhaustivo de documentación. Como expresamos anteriormente, la documentación sirve simultáneamente para tres propósitos: adquirir conocimientos sobre el campo temático, lograr el dominio de la terminología propia del mismo, y obtener información sobre las normas de funcionamiento del género. Los tres factores hacen necesario que el traductor se documente antes de realizar su trabajo, y que lo haga de una forma amplia y suficiente, en función de sus conocimientos y de la dificultad del texto, e integrando los tres objetivos cuando sea posible, con el fin de rentabilizar el proceso.

Una tercera dificultad estribó en tener en cuenta los procedimientos de adaptación. Es preciso destacar la vertiginosa velocidad a la que avanzan las nuevas tecnologías y, por consiguiente, la nueva terminología. Como consecuencia inmediata, el español se ve obligado a importar esta nueva terminología del inglés. Una de las posturas más cómodas por parte del traductor es mantener el término en inglés, aunque ello no quiera decir que sea la opción más correcta. En primer lugar, habría que determinar si un neologismo ya se ha integrado y ha dejado de serlo. Por lo tanto, el primer procedimiento de adaptación de los textos técnicos es el uso de anglicismos, que no siempre es responsabilidad del traductor, sino de los redactores técnicos, las instituciones o las empresas. No obstante, en algunas ocasiones, el traductor se encuentra con que algunos de los términos que debe traducir ya se han integrado en la lengua de destino a pesar de que no sea la mejor opción de traducción. En esos casos, este debe adaptarse a la terminología que se emplea asiduamente en el campo especializado.

El grado de especialización en la materia también resulta importante, ya que con la práctica profesional el traductor va adquiriendo un completo bagaje cultural relacionado con los ámbitos de las traducciones que realiza. Por eso, a

la larga acaba especializándose en unos temas concretos. No obstante, dada la situación económica actual, siempre debe estar abierto a nuevas temáticas y, por lo tanto, a documentarse y a estar al día en todo lo posible. En definitiva, el traductor debe poseer una gran cultura general que le permita adaptarse y documentarse a nuevas tipologías textuales.

El libro de J. Byrne (2006) *Technical Translation: Usability Strategies for Translating Technical Documentation* es verdaderamente esclarecedor a la hora de esclarecer algunas afirmaciones erróneas que, hasta la fecha, se han realizado en torno a la traducción técnica y, por ende, en torno a la traducción de textos pertenecientes al sector de las comunicaciones.

En primer lugar, se destaca la importancia de la traducción técnica, que supone el 90% de las traducciones que se llevan a cabo cada año a nivel mundial. A pesar de su abrumadora demanda, existen multitud de mitos arraigados sobre la importancia, la naturaleza y el papel de la traducción técnica tanto en el entorno profesional, como el académico.

1. **La traducción técnica incluye economía, derecho, negocios, etc**. En realidad, "técnica" significa precisamente eso, algo relacionado con la tecnología y los textos tecnológicos.
2. **La traducción técnica solo tiene que ver con la terminología**. Esta afirmación errónea está extendida incluso entre personas que están involucradas en el mundo de la traducción técnica, por ejemplo, Pinchuck (1977), quien afirma que el vocabulario es lo más importante. Sin embargo, más importante que la terminología es en realidad saber cómo escribir un texto. Según Lee-Jahnke (1998: 83-84), hay tres cosas esenciales para tratar con los textos científicos y técnicos: conocer la estructura textual en diferentes idiomas, conocer la terminología y conocer el tema.
3. **El estilo no es importante para la traducción técnica**. Para el autor, el estilo, que se ha considerado la mejor manera de garantizar el cumplimiento de las normas del idioma meta, puede tener en realidad efectos mucho más profundos en la calidad de las traducciones técnicas.
4. **La traducción técnica no es creativa, es simplemente un proceso reproductivo de transferencia**. No obstante, para conseguir información de forma apropiada y efectiva, los traductores técnicos tienen que encontrar

soluciones lingüísticas novedosas y creativas para asegurar el éxito de la comunicación.

5. **Hay que ser un experto en un tema altamente especializado**. Sin embargo, está demostrado que un traductor técnico que obtenga un claro entendimiento de las bases de la ciencia y la tecnología puede proporcionar un buen fundamento para diversas aplicaciones dentro de la traducción técnica.

6. **La traducción técnica solo consiste en conseguir información especializada**. El traductor técnico no solo tiene que documentarse para obtener información especializada, además debe conocer en detalles las culturas de los idiomas origen y meta, las convenciones textuales del idioma de destino, las características del género y el tipo de texto, el registro, el estilo, un detallado conocimiento de los receptores, y, con independencia de que el traductor sea consciente de ello o no, un entendimiento de cómo las personas aprenden y utilizan la información.

5.2. Búsqueda documental

La búsqueda documental tiene especial importancia para el traductor porque esta resuelve sus carencias en el ámbito temático, terminológico y de géneros. Esta competencia es con toda probabilidad una de las más importantes. El proceso de documentación tiene tres propósitos principales:

* Adquirir conocimientos sobre el campo temático.
* Lograr el dominio de la terminología propia del mismo.
* Obtener información sobre las normas de funcionamiento del género.

Para cumplir estos propósitos es necesario que el traductor lleve a cabo una búsqueda documental antes de realizar su trabajo de forma amplia y suficiente de acuerdo con su propio bagaje y con la dificultad del texto. Lo ideal es integrar estos tres objetivos siempre que sea posible con el propósito de sacar el máximo partido al proceso. El dominio de la documentación como herramienta de trabajo implica, por un lado, conocer las obras de referencia disponibles y saber utilizarlas y, por el otro, ser capaz de aplicar una metodología adecuada para localizar rápidamente, evaluar y acceder a las

fuentes de información más apropiadas en cada caso, así como para extraer los datos necesarios de ellas en el mínimo tiempo necesario.

La búsqueda documental es de especial importancia para localizar las convenciones de los géneros textuales, tanto en lengua de partida como de llegada. Por ejemplo, en el caso de la traducción de una patente técnica británica, el texto de llegada tendrá que atenerse a las normas marcadas por la legislación española para la presentación de solicitudes, que son muy estrictas. Con la documentación, obtendremos información sobre el funcionamiento del género, ya que el texto consultado en lengua de llegada ha de pertenecer al mismo género que el texto de partida. En este caso, la habilidad consiste en ser capaz de identificar y localizar los textos paralelos dentro de la documentación especializada y saber extraer los rasgos típicos.

En la actualidad, no podemos dejar de mencionar la creciente utilidad de Internet, que pone a disposición del traductor tanto fuentes documentales como bibliográficas y terminológicas. Este ha de saber utilizar las herramientas de búsqueda adecuadas y conocer los métodos de evaluación de la información ofrecida, que se rige por unos criterios específicos, como son la autoría, contenido, acceso y diseño (Palomares, 1999: 179).

5.3 Problemas terminológicos y documentales

El traductor debe solucionar los problemas de índole terminológica[31] y documental, de modo que pueda entregar un texto meta adecuado. No se trata de que una tipología sea más complicada que otra, ya que la complejidad dependerá del caso concreto que nos ocupe.

A continuación, analizaremos algunos ejemplos de problemas de índole documental y terminológica extraídos de *CompTIA Security +.*

5.3.1 Contextualización de la temática

En el caso del manual objeto de estudio hemos de reseñar que la introducción del libro fue fundamental a la hora de contextualizar su temática:

[31] De gran interés y utilidad resulta la obra de S. Pavel y D. Nolet: *Handbook of Terminology.* Ottawa: Public Works and Government Services Canada, 2001.

Introducción

Si se está preparando para presentarse al examen Security+, no cabe ninguna duda de que está interesado en encontrar el máximo de información posible relacionada con la informática y la seguridad física. Cuantos más datos tenga a su disposición y mayor experiencia adquiera, mejor preparado estará para enfrentarse al examen. Esta guía de estudio está redactada con esa idea. El objetivo es proporcionar suficiente materia para cubrir el temario del examen, pero no demasiada y sobrecargarle con información que esté fuera del ámbito de la prueba.

Este libro presenta el material en un nivel técnico intermedio. Todos los conocimientos y experiencia que tenga relación con conceptos de seguridad, sistemas operativos y de aplicación le serán útiles para ser totalmente consciente de los retos a los que se enfrentará como profesional de la seguridad.

Se han incluido cuestiones de repaso al final de cada capítulo para que tenga una idea de las preguntas del examen. Si ya ha trabajado en el campo de la seguridad, es recomendable que compruebe primero las preguntas con el fin de determinar el nivel de sus competencias. A continuación, utilice el libro para cubrir las lagunas de su formación actual. Esta guía de estudio le ayudará a completar su base de conocimiento antes de presentarse al examen.

Si puede responder al 90 por ciento o más de las preguntas de repaso en un capítulo, no dude en pasar a otro. Si, por el contrario, no puede responderlas de forma correcta, reléalo y vuelva a intentarlo. Su puntuación debería mejorar.

Para abordar un proyecto de traducción de este tipo, el traductor debe tener unas claras nociones de informática en general. De lo contrario, le será realmente difícil entender la temática del texto y todos los términos y conceptos que este incluye. Aunque pueda recurrir a una búsqueda documental, sin un bagaje previo por parte del traductor, esta sería realmente extensa y compleja.

5.3.2 Localización de la tipología de un campo concreto

Un claro ejemplo de problema documental es la localización de toda la tipología de un campo concreto; por ejemplo, uno de los campos que tuvimos que investigar fue el de los tipos de virus informáticos:

Virus: Programa que pretende causar daños en un ordenador. Los virus más sofisticados están cifrados y se ocultan en un ordenador. Puede que no aparezcan hasta que el usuario lleve a cabo alguna acción o hasta una fecha específica. Véase también Antivirus.

Virus acompañante: Virus que crea un nuevo programa que se ejecuta en lugar del programa esperado con el mismo nombre.

Virus blindado: Un virus blindado está diseñado para que sea difícil detectarlo o analizarlo. La dificultad recae en que este puede estar escrito de tal modo que algunos programas tengan problemas para acceder y entender su código.

Virus de macro: Virus de explotación de software que funciona utilizando la característica macro que incluyen muchas aplicaciones.

Virus fagocito: Virus que modifica y altera otros programas y bases de datos.

Virus invisible: Virus que intenta evitar la detección enmascarándose desde las aplicaciones.

Virus múltiple: Virus que ataque a un sistema de varias maneras.

Para resolver este problema el traductor debe realizar una búsqueda documental en fuentes fiables y traducir de forma adecuada cada tipo de virus según las convenciones de utilización en la lengua meta. En su tesis doctoral[32] Cordón García (2002) trata el tema de los problemas documentales desde distintas perspectivas. Otra de sus obras[33] abarca esta temática desde una panorámica más actual en la que las fuentes documentales han evolucionado y, por lo tanto, los problemas documentales se resuelven teniendo en cuenta estos avances (Cordón García *et al*., 2012).

Para recopilar este tipo de información tan especializada, hemos recurrido a monografías[34] realizadas por expertos del sector. En contraposición

[32] J. A. CORDÓN GARCÍA: *Bibliografías nacionales y Depósito Legal: un problema documental*. Ediciones Universidad de Salamanca, 2002.

[33] J. A. CORDÓN GARCÍA, J. ALONSO AREVALO, R. GÓMEZ DIAZ y J. LOPEZ LUCAS. *Las nuevas fuentes de Información: información y búsqueda documental en la Web 2.0.* 2º Edición, corregida y aumentada. Madrid, Pirámide, 2012.

[34] V. ACEITUNO. *Seguridad de la Información*. Creaciones Copyright, 2004.
P. AGUILERA. *Seguridad informática*. Editex, 2010.
J. AREITO. *Seguridad de la información redes, informática y: sistemas de información*. Madrid: Paraninfo, 2008.

a otros campos del saber, uno de los elementos fundamentales que hemos de tener en cuenta para traducir proyectos del sector de la seguridad informática es la actualidad de las fuentes documentales, ya que como hemos mencionado con anterioridad se trata de un sector que evoluciona rápidamente. Más aún en el caso de los virus informáticos, que están en constante movimiento, apareciendo y desapareciendo de forma constante.

5.3.3 La traducción de siglas

La traducción de siglas es, en el caso que nos ocupa, un problema de índole conceptual y terminológica que también requiere de una búsqueda documental. Además, el traductor debe adaptar su presentación a las especificaciones de la editorial que publicará el libro en lengua meta. Ofrecemos algunos ejemplos de siglas que aparecen en nuestro manual:

ACK (*Acknowledgment*, reconocimiento): Mensaje que confirma que se ha recibido un paquete de datos. El reconocimiento es una función de TCP que se produce en la capa Transporte de los modelos OSI (*Open Systems Interconnection*, Interconexión de sistemas abiertos) y TCP/IP.

ACL (*Access Control List*, Lista de control de acceso): Tabla o archivo de datos que especifica si un usuario o grupo de ellos tiene acceso a un recurso específico del ordenador o de la red.

AD-IDS (*Anomaly-detection IDS*, IDS de detección de anomalías): Funciona buscando anomalías en los patrones de tráfico de red habitual.

AES (*Advanced Encryption Standard*, Estándar de cifrado avanzado): Publicación de FIPS que especifica el algoritmo criptográfico que utiliza el gobierno de los EE.UU. Véase también FIPS (*Federal Information Processing Standard*, Estándares Federales de Procesamiento de la Información).

AES256: Implementación del Estándar de cifrado avanzado (AES) que utiliza un cifrado de 256-bits.

AH (*Authentication Header*, Encabezado de autenticación): Encabezado que se utiliza para proporcionar integridad sin conexión

M. OROSCO. (et al*). Informática 1.* México: Thompson, 2006.
J. M. ROYER. *Seguridad en la informática de empresa.* Barcelona: Ediciones ENI, 2004.

> y autenticación del origen de los datos para los datagramas IP y para ofrecer protección frente a reproducciones.
>
> **ALE (*Annualized Loss Expectancy*, Expectativa de pérdida anualizada):** Cálculo que se utiliza para identificar los riesgos y calcular las pérdidas esperadas para cada año.[35]

En cuanto a la traducción de siglas, Pérez Berenguel (2003: 622)[36] afirma que el criterio recomendable en todos los libros de estilo es el de la traducción de los términos y de la reordenación de sus siglas, siempre y cuando tengan una traducción aceptada ampliamente en las diferentes lenguas de destino. Sin embargo, existen otras siglas que hacen referencia a estándares establecidos que se han erigido como marcas muy conocidas del sector (W3C, *World Wide Web Consortium,* Consorcio World Wide Web) y que, por lo tanto, no se traducen y se emplean en el orden en el que aparecen en la lengua de origen. A la hora de decidir nuestras estrategias de traducción hemos de tener en cuenta todos estos factores.

Por otro lado, la creciente globalización en el ámbito de la informática conlleva una tendencia cada vez mayor a la estandarización terminológica. Sin embargo, aunque esta tendencia globalizadora ha suprimido algunos problemas de traducción (VPN, *Virtual Private Network,* Red privada virtual), algunas siglas sí que se traducen y mantienen sus singularidades, ya que su uso se remonta atrás en el tiempo y en el uso común se llevan traduciendo desde su introducción en el lenguaje español. Por ejemplo, SO (Sistema operativo) en lugar de OS (Operating System).

5.4 Estrategias de traducción

El traductor dispone de distintas técnicas cuando la búsqueda terminológica resulta infructuosa. En las búsquedas terminológicas de tipo puntual, el traductor requiere el equivalente de un término concreto en lengua

[35] Fuente: IBM Knowledge Center: Tipos de cifrado y modalidades de cifrado. <http://www.ibm.com/support/knowledgecenter/es/SSGU8G_12.1.0/com.ibm.sec.doc/ids_en_010.htm> [Fecha de consulta: 13 de diciembre 2016]

[36] J. F. Pérez Berenguel. "Glosario de errores comunes en la traducción económica y financiera". En R. Muñoz Martín (ed.) *I AIETI. Actas del I Congreso Internacional de la Asociación Ibérica de Estudios de Traducción e Interpretación*. Granada 12-14 de Febrero de 2003. Granada: AIETI, pp. 619-628.

de llegada. El método consiste en consultar una obra de referencia de tipo terminológico; en este caso, el traductor ejerce de usuario de la terminología. Por otra parte, en las búsquedas de tipo sectorial, se centra en un conjunto de términos en un ámbito técnico concreto. Su papel es más activo y recurre a la documentación por medio de textos especializados, lo que le permite obtener una lista de términos relativos al campo concreto con el que está trabajando.

Otra vía que puede resultar fundamental es la consulta a especialistas, siempre que se aplique la estrategia adecuada, realizando preguntas concretas y situándolas en un dominio determinado. Huelga decir que el propio traductor debe ir adquiriendo un bagaje terminológico a través de la lectura asidua de textos técnicos que aparecen en la prensa general o especializada y en los anuncios técnicos.

No obstante, si esta búsqueda terminológica resulta infructuosa, porque la equivalencia entre lenguas es parcial o nula, el traductor dispone de tres técnicas para solucionar el problema: préstamo, neologismo o paráfrasis (como señalábamos en el apartado 4.2.4). Cuando se decide por alguna de las dos primeras, idealmente debe consultar a un especialista en terminología, ya que la aparición de préstamos y neologismos no controlados supone un peligro para la armonización internacional de los términos, y al mismo tiempo favorece la excesiva proliferación de sinónimos.

Por otra parte, cabe destacar brevemente algunas posturas relacionadas con los procesos de resolución de problemas. Un punto clave en los estudios sobre los procesos de resolución de problemas es el carácter estratégico que deben poseer con el fin de conseguir una mayor efectividad. De acuerdo con Pozo *et al*. (1994: 37):

> …la solución de problemas requiere que el entrenamiento técnico se complemente con un conocimiento estratégico que permita utilizar esas técnicas de modo deliberado en el contexto de tareas o situaciones abiertas, que admiten soluciones diversas, a las que llamamos problemas.

En este sentido, los mismos autores afirman que numerosos estudios relacionados con los procesos de resolución de problemas han demostrado que “los expertos no solo son más rápidos y cometen menos errores en la solución de problemas sino que, sobre todo, adoptan estrategias diferentes a las empleadas por los novatos” (1994: 39). A partir de estas investigaciones, realizadas en su mayor parte con problemas bien definidos, se desprende que

los expertos suelen invertir menos tiempo en la resolución de un problema de su campo de conocimiento porque reconocen con más facilidad el problema como una situación conocida, con lo que, de modo más o menos automático, establecen, siguiendo la terminología de Polya (1945), el plan de acción adecuado que ejecutan con rapidez y eficacia.

En relación con la adquisición de destrezas específicas en una determinada materia, Anderson (1983) afirma que la solución experta de un problema implica la conversión de un conocimiento verbal o declarativo, consistente en instrucciones o reglas, en una secuencia de procedimientos ejecutados de forma rápida y automatizada, o dicho de otro modo, implica llegar a convertir un tipo de conocimiento declarativo en un conocimiento de tipo operativo.

Esto resulta vital para nuestra profesión, ya que lo que se pretende al estudiar estos procesos estratégicos y los operadores que los constituyen es precisamente llegar a hacer declarativo un proceso eminentemente operativo. Sin embargo, el camino hacia una definición precisa de lo que constituye ese conocimiento operativo no está exento de obstáculos (debidos principalmente a la dificultad que supone acceder a los procesos que tienen lugar en la mente humana), de ahí el que muchos intentos de verbalizar estos procesos automáticos y no verbales no hayan logrado su propósito.

Al retomar la distinción de Polya (1945) entre procesos heurísticos y procesos algorítmicos de resolución de problemas, Pozo *et al.* (1994: 40) afirman que “la solución experta de problemas se basa en gran medida en la aplicación de procedimientos técnicos, más que en el uso deliberado e intencional de estrategias”. Sin embargo, esta automatización de técnicas, producto de la práctica, dicen, permite liberar recursos cognitivos que hacen que la conducta experta sea también más eficaz cuando se enfrenta a “verdaderos problemas”, es decir, a situaciones que no pueden ser fácilmente reducidas a categorías ya conocidas. La ventaja de los expertos en ese proceso estratégico (es decir, no automatizado) parece residir en el mayor control que ejercen sobre sus procesos de solución.

Esta distinción entre procedimientos técnicos y estrategias nos lleva a una de las cuestiones centrales en los estudios sobre los operadores del proceso traductor. Técnicas, procedimientos, procedimientos técnicos, estrategias son términos que o bien reciben un mismo tratamiento, o bien

vienen a referirse a conceptos bien distintos. La distinción de Pozo *et al.* (1994), en este sentido, deberá servirnos de punto de partida para comprender mejor la verdadera tipología de operadores que actúan durante el proceso de traducción, sin por ello olvidar que estamos hablando de un mismo tipo de conocimiento. En este sentido, podemos decir que los operadores del proceso traductor, en la forma que fuere, son fundamentales para la resolución de problemas y, en consecuencia, fundamentales para la competencia traductora. A continuación ofrecemos algunos ejemplos de estas técnicas o estrategias de traducción que se emplean cuando la búsqueda terminológica resulta infructuosa. Están extraídas de la traducción propia de *CompTIA Security* +, objeto de estudio en el presente trabajo:

* **Préstamo:** Bajo el nombre de préstamos puros se agrupan algunas voces que han sido adoptadas directamente del inglés. Aunque se suelen mantener (por lo menos en su forma escrita) fieles al término original, pueden también adaptarse a las normas fonomorfológicas del español y muestran, en mayor o menor medida, un reflejo de la pronunciación original (Montero Fleta, 2004). En opinión de García Yebra (1989: 334), el préstamo trata de llenar una laguna en la lengua receptora, laguna generalmente relacionada con una técnica nueva, con un concepto desconocido entre los hablantes de esta lengua. La asimilación del vocablo inglés por parte del español es total. Generalmente se trata de conceptos nuevos que también en inglés han sido acuñados o han ampliado su significado para dar nombres a conceptos inexistentes. Algunos ejemplos de préstamos dentro de nuestro corpus son los siguientes:

> "Para que funcione, Evan tendría que haber accedido recientemente al sitio Web del banco y tener una cookie que todavía no haya expirado."
>
> (pág. 6, archivo .doc 07)
>
> **Cookie**: Archivo de texto simple almacenado en su máquina que contiene información sobre usted (y sus preferencias) y puede utilizarlo el servidor.

* **Calco:** Es un anglicismo semántico, ya que afecta a un significado perfectamente atendido por una palabra española original (Montero Fleta, 2004); la influencia opera en este caso en lo que se refiere a la semántica. Como señalara García Yebra (1989: 343): "El calco tiene la

ventaja de hacer que los lenguajes técnicos resulten fácilmente comprensibles para hablantes no especializados". Sin embargo, pensamos que algunos no responden más que a una mala o precipitada traducción, como también señalan Montero *et al*. (1993). Veamos algunos ejemplos de nuestro corpus:

> Loop protection is a similar feature that works in layer 2 switching configurations and is intended to prevent broadcast loops. When configuring it in most systems, you can choose to disable broadcast forwarding and protect against duplicate ARP requests (those having the same target protocol address).
>
> (pág. 411, libro original)
>
> La protección del bucle es una característica similar que funciona en la capa 2 de las configuraciones de conmutación y está ideada para evitar los bucles de difusión. Cuando se configura en la mayoría de los sistemas, puede preferir deshabilitar la transferencia de difusión y establecer una protección frente a las solicitudes ARP duplicadas (las que tienen la misma dirección de protocolo de destino).
>
> (pág. 5, archivo 11.doc)

> *Risks Associated with Cloud Computing*
>
> (pág. 7, libro original)
>
> Riesgos asociados a la computación en nube
>
> (pág. 4, archivo 11.doc)
>
> Hace poco tiempo que la popularidad del término computación en nube ha empezado a crecer, pero muy pocos se ponen de acuerdo a la hora de determinar qué significa en realidad.
>
> (pág. 4, archivo .doc 01)

* **Neologismo:** Los neologismos son voces nuevas a partir de elementos preexistentes, mediante la necesaria adaptación semántica, o pueden resultar creaciones totalmente nuevas y originales (Montero Fleta, 2004: 46). Su creación puede responder a una necesidad real, ya que son términos que hacen referencia a inventos, procesos o máquinas nuevas. No obstante, en ocasiones, son claramente injustificados, ya que aunque existe una palabra equivalente en la lengua española, se recurre al término inglés, llegando a adaptarlo según las pautas ortográficas, morfológicas y fonológicas del español.

La terminología específica del mundo de la informática presenta un cuerpo abundante de neologismos (ej. inicializar, organigrama, etc). Hay que tener en cuenta que al utilizar un neologismo, debemos aseguramos de que nos aporta más claridad y precisión que cualquier palabra ya consagrada en nuestro léxico. Analicemos algunos ejemplos localizados en nuestro corpus:

"En una LAN, los host pueden comunicarse entre sí utilizando las difusiones y no necesitan dispositivos de reenvío, como enrutadores."

(pág. 7, archivo .doc 05)

Enrutador: Un dispositivo que conecta redes separadas, que reenvía un paquete de una red a otra basándose solo en la dirección de red del protocolo que se está utilizando. Un enrutador determina la mejor ruta para los paquetes de datos desde el origen a su destino.

* **Paráfrasis:** En general, se suele evitar la paráfrasis en la medida de lo posible y prima la utilización de las dos técnicas anteriores siempre que no haya una posible traducción del término en cuestión para otorgar al texto de mayor rigor científico y técnico, ya que la terminología es uno de los factores determinantes en la esencia del lenguaje técnico.

Right-click the network you are connected to and choose Properties.

(pág. 4, libro original)

Haga clic con el botón derecho del rato en la red a la que está conectado y seleccione Propiedades.

(pág. 6, archivo 12.doc)

6. PROYECTO TERMINOLÓGICO

Este capítulo se divide en tres partes fundamentales para el presente trabajo de investigación: el fichero terminológico de 165 fichas, el glosario bilingüe (inglés-español) con los términos seleccionados y una muestra del sistema de conceptos. A partir de este trabajo se elaboró una base de datos terminológica en Excel que, posteriormente, se exportó a Multiterm para utilizarla en Trados.

6.1 Diseño del fichero terminológico

Una de las cuestiones más relevantes a las que la terminología moderna debe hacer frente de forma ineludible es la reutilización de la información terminológica. No cabe duda de que todas las empresas que tienen como objetivo la recopilación y organización de información, sea esta del tipo que sea, deben plantearse desde un principio qué garantías presenta ese cuerpo de información a la hora de ser reutilizado en empresas para las que inicialmente no fue concebido (Pérez Hernández, 2002)[37]. En algunos ámbitos de investigación, tales como el de las bases de datos y sistemas de información en general, este aspecto es, junto con el de la seguridad y coherencia de los datos, al que más tiempo se le ha dedicado en las últimas tres décadas (Gardarin y Valduriez, 1989).

Dada la elevada densidad terminológica del texto que se analiza en este trabajo, la realización de un fichero terminológico bilingüe formado por un total de **ciento sesenta y cinco** clasificadas en categorías ha sido una de las fases más relevantes de esta investigación. Además, con el propósito de completar este fichero, se incluye también un glosario igualmente bilingüe que incluye el mismo número de entradas.

[37] Véase también:

M. CHANTAL PÉREZ HERNÁNDEZ: "Explotación de los córpora textuales informatizados para la creación de bases de datos terminológicas basadas en el conocimiento". *Estudios de Lingüística del Español (ELiEs).* Universidad de Málaga, 2002.
URL: <http://elies.rediris.es/elies18/index.html> [Fecha de consulta: 30 de agosto , 2015].

G. GARDARIN Y P. VALDURIEZ: *Relational Databases and Knowledge Bases*. Reading, Mass: Addison-Wesley, 1989.

Para la elaboración de las fichas nos hemos basado en las Categorías de datos de la norma ISO 12620 y su aplicación.

Las categorías de datos propuestas por el comité técnico 37 de la ISO tomadas por el CLS Framework han sido agrupadas en diez subcategorías que se complementan con dos grupos de categorías de la norma ISO 12200 (el estándar MARTIF, del que nos ocuparemos en el apartado 5.5.4). Estas categorías se resumen en el cuadro siguiente adaptado de Wright (en prensa /b: 574):

ISO 12620: GRUPOS DE CATEGORÍAS DE DATOS
Categorías de datos relacionadas con el TÉRMINO
Subgrupo 1: Categoría de datos término y contiene un término u otra información tratada como tal (ej. una unidad fraseológica o un texto estándar).
Subgrupo 2: Categorías de datos que contienen información sobre el término.
Subgrupo 3: Categorías de datos sobre la equivalencia entre términos asignados al mismo concepto o a conceptos similares.
Categorías de datos descriptivas, relacionadas con el CONCEPTO
Subgrupo 4: Categorías de datos que clasifican los conceptos en áreas o subáreas temáticas.
Subgrupo 5: Categorías de datos para la descripción del concepto, por ejemplo, diferentes tipos de definiciones, explicaciones o material contextual usado con el fin de definir el concepto o para determinar el área temática y el concepto al que se asigna un término.
Subgrupo 6: Categorías de datos que indican relaciones entre dos conceptos.
Subgrupo 7: Categorías de datos que se usan para indicar la posición de los conceptos en un sistema conceptual.
Subgrupo 8: Categoría de datos nota. Esta categoría aparece aislada ya que puede asignarse a cualquier otra categoría y por tanto no puede subordinarse a ningún grupo específico.
Categorías de datos ADMINISTRATIVAS (gestión)
Subgrupo 9: Categorías de datos de los lenguajes documentales y tesauros.
Subgrupo 10: Categorías de datos de la información de gestión y administrativa.
ISO 12200: CATEGORÍAS DE DATOS SUPLEMENTARIAS
Subgrupo 11: Especifica los códigos especiales usados en el estándar MARTIF.
Subgrupo 12: Especifica las categorías de datos para la información bibliográfica.

Tabla 8. Grupos de categorías de datos.

Estos diez subgrupos engloban un total de más de 150 categorías de datos que, a juicio de los miembros del comité técnico de la ISO, no pretenden ser exhaustivas. Tampoco se pretende en el CLS Framework que una base de datos incluya todas y cada una de estas categorías, sino solo las que se consideren necesarias para representar la información pertinente a un proyecto terminológico determinado.

Según la norma ISO 12620, una ficha terminológica tipo deberá contener la siguiente información:

<table>
<tr><td>10.16. Record identifier</td><td>2.1.1. Main entry term</td><td>10.20. Source identifier</td><td>10.7. Language symbol (ISO 639)</td></tr>
<tr><td colspan="4">2.2.1. Part of speech</td></tr>
<tr><td colspan="4">4. Subject field
Level 1
Level 2
Level 3</td></tr>
<tr><td colspan="3">5.1. Definition</td><td>10.20 Source identifier</td></tr>
<tr><td colspan="3">5.3. Context</td><td>10.20. Source identifier</td></tr>
<tr><td colspan="2">3.1. Equivalent</td><td>10.20 Source identifier</td><td>10.7. Language symbol (ISO 639)</td></tr>
<tr><td colspan="3">10.2.1.1. Origination date</td><td>10.2.2.1. Originator</td></tr>
</table>

Figura 14. Modelo de ficha terminológica.

Por otra parte, la norma ISO 12200: MARTIF (*Machine-Readable Terminology Interchange Format*) ha sido desarrollada con la finalidad de facilitar el intercambio de recursos terminológicos en formato electrónico.

En resumen, el objetivo de MARTIF es convertirse en "el RTF de las bases terminológicas". De este modo, al igual que su homólogo textual, MARTIF pretende servir de "interlingua" terminológica, garantizando el intercambio entre usuarios (individuos o corporaciones) que utilizan software y hardware dispares.

Tras la documentación sobre fichas terminológicas y la adaptación a este proyecto concreto, realizamos unas fichas específicas para este trabajo. El diseño de las fichas pretende ofrecer una interpretación clara y sencilla a los

usuarios. Por ello, solo se han seleccionado campos que aportaran información precisa y relevante tras un exhaustivo proceso de elaboración. A continuación, se señalan los campos que incorpora cada una de las fichas y una breve descripción de su función.

- **Identificación**: Número, iniciales del autor y fecha de elaboración.
- **Término en inglés**: Aparece el término extraído del documento original.
- **Referencia**: Fuente donde aparece el término original. Solo aparece la referencia completa en la primera ficha. En el resto del fichero, la referencia al corpus de estudio se hace de forma abreviada.
- **Traducción**: Término traducido al castellano. Dada la variedad de términos que aparecen en el texto objeto de análisis, se han empleado multitud de estrategias de traducción (préstamos, neologismos, etc).
- **Fuente de la traducción**: Fuente en la que se ha localizado el término equivalente en español.
- **Definición**: Definición del término en castellano. El análisis de este texto se ha adaptado en todo momento a las particularidades del mismo. Prueba de ello es que las definiciones recogidas en las fichas son las que aparecen en el propio glosario del texto meta que, a su vez, son una traducción de la definición que aparece en el glosario del texto original.
- **Fuente de la definición**: Fuente en la que se ha localizado la definición del concepto.
- **Observaciones**: Todo aquello que merezca mención aparte y no quede reflejado en ninguno de los campos que aparecen con anterioridad. En caso de no haberlas, se indica N/A (No Aplicable).

A continuación, presentamos el modelo de ficha que hemos empleado en este trabajo de investigación.

FICHA Nº XX	AUTOR Y FECHA
TÉRMINO	REFERENCIA
EQUIVALENTE	
DEFINICIÓN	
FUENTE DE LA DEFINICIÓN[38]	
OBSERVACIONES	

Tabla 9. Modelo de ficha utilizado en el proyecto terminológico.

Por último, hemos de destacar que, debido a la densidad terminológica de este texto, las fichas aparecen clasificadas en cuatro categorías de acuerdo con la estrategia que se ha seguido para su traducción. De este modo, resulta más fácil su categorización e interpretación. Es así como el usuario puede encontrar los siguientes apartados:

1. Neologismos
2. Préstamos y calcos
3. Siglas y acrónimos
4. Traducción por equivalencia

Sin duda, esta clasificación ha facilitado en gran medida la obtención de una perspectiva general de las estrategias de traducción que se han empleado. Además, ha facilitado la ordenación de los términos para llevar a cabo el complejo análisis terminológico.

No obstante, dado el carácter eminentemente práctico de este trabajo de investigación, a efectos de organización y eficacia, decidimos estructurar el trabajo de la siguiente manera:

1. En primer lugar, los términos se clasifican en la siguiente tabla por neologismos, préstamos y calcos y traducción por equivalencia y, a su vez, por orden alfabético. Cada columna está caracterizada por un color que se utilizará en las fichas del proyecto terminológico para saber en todo momento a qué categoría pertenece cada ficha.

[38] *Fuente de la definición*: En este caso, tanto la Fuente de la definición como la Fuente de la equivalencia proceden de la misma fuente documental con el fin de simplificar el proceso, dado que el objetivo primordial es crear una base de datos terminológica de cara a una traducción profesional.

2. Las fichas terminológicas aparecen en orden alfabético dado que su fin último es convertirlas en un glosario en Excel y exportarlo a Multiterm. En nuestro caso, la esencia del presente trabajo de investigación es llevar el análisis terminológico a la práctica y, aunque hemos querido reflejar la categoría de los términos en las fichas, consideramos que lo más efectivo es ordenarlas alfabéticamente para realizar la base de datos en Multiterm.

A continuación, aparece la tabla de clasificación de los términos diferenciada por colores y en orden alfabético.

Neologismos	Préstamos y calcos	Siglas y acrónimos	Traducción por equivalencia
authentication	adware	ACL	access control
biometrics	bastion host	BPN	add-on
biometrics devices	bit	CAC	algorithm
buffer	bot	CCTV	attachment
datagram	cookie	CHAP	attack
digital	cross-site scripting	CIA	authorization
encryption	Ethernet	DAC	broadcast
extrusion	Extranet	DMZ	buffer overflow
firewall	hacker	DNS	client
gateway	honeynet	DSSS	common access card
host	honeypot	EMI	identification
hub	Internet	FHSS	implicit deny
modem	Intranet	FTP	link
multicasting	Kerberos	FTPS	load balancers
partitioning	login	HTTP	MAC address
password	logon	HTTPS	malicious add-ons
port scanner	mantrap	HVAC	mandatory access control
router	multihoming	IANA	network
scanning	ping	ICMP	network segmentation
server	proxy	IDS	PBX system

single sign on	roaming	IEEE 802.11x	perimeter
standard	roaming profile	IP	personal identification verification card
tunneling	role/rule-based access	IPS	physical barriers
virtualization	script	IPSec	polymorphic
	scripting	IPv4	protocol
	sniffer	IPv6	protocol analyzer
	spam filter	IPX	remote access
	subnetting	ISDN	secure copy
	switch	ISP	security server
	token	L2TP	security topology
	zombie	LAN	security zone
		LDAP	seven-layer OSI model
		MAC	signal
		NAC	smart card
		NAT	smart card reader
		NCP	social engineering
		NetBIOS	spike
		NIC	topology
		NIDS	thelephony
		NIPS	
		OSI model	trusted OS
		PPP	user
		PPTP	VPN concentrators
		RADIUS	web security gateways
		SCP	wireless access point
		SFA	zone
		SFTP	
		SNA	
		SNMP	
		SSH	
		SSL	

		TACACS	
		TACACS+	
		TCP	
		TCP/IP	
		TELNET	
		TKIP	
		TLS	
		UDP	
		UPS	
		VLAN	
		VPN	
		WEP	
		Wi-Fi	
		WPA	
		WTLS	
		XTACACS	

Tabla 10. Modelo de ficha utilizado en el proyecto terminológico.

Por último, presentaremos las fichas terminológicas. Nos gustaría recordar que nos hemos decantado por este tipo concreto de ficha debido a las especificidades del encargo y al hecho de que el objetivo primordial de la creación de este fichero terminológico es el de volcarlo en una base de datos terminológica (SDL Multiterm 2014) para integrarlas con SDL Trados 2014 y sistematizar el proceso de traducción.

6.2 Fichero terminológico[39]

FICHA Nº 1	AUTOR Y FECHA MJPM, 2 de septiembre, 2014
TÉRMINO **access control**	**REFERENCIA** E. DULANEY: *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. Hoboken, NJ: Hoboken, NJ: Wiley Publishing, Inc. EE.UU. 2011.
EQUIVALENTE	**control de acceso**
DEFINICIÓN Medios para permitir o restringir el acceso a los usuarios para utilizar los recursos de una red. El control de acceso se suele llevar a cabo empleando una ACL (Access Control List, Lista de control de acceso).	
FUENTE DE LA DEFINICIÓN Glosario. E. DULANEY: *Seguridad Informática. CompTIA Security+* (Títulos Especiales). Madrid: Editorial Anaya Multimedia, 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 2	AUTOR Y FECHA MJPM, 2 de septiembre, 2014
TÉRMINO **ACL**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**ACL**
DEFINICIÓN *Access Control List*, Lista de control de acceso. Tabla o archivo de datos que especifica si un usuario o grupo de ellos tiene acceso a un recurso específico del ordenador o de la red.	

[39] Previo al proceso de traducción, se procedió a la traducción del glosario que incluye el propio manual. Para ello, se realizó la correspondiente labor documental. Es por esta razón que incluimos las definiciones del propio glosario ya traducidas, primando así la coherencia y la sistematicidad.
Se mantiene la numeración de las fichas en el orden de creación, como muestra de la evolución del fichero terminológico y se sitúan en orden alfabético.

FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 105	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **add-on**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**complemento**
DEFINICIÓN Dispositivo que se añade a la base del sistema informático para incrementar su funcionalidad, por ejemplo, audio, red, gráficos o controladores SCSI.	
FUENTE DE LA DEFINICIÓN Microsoft Office - Portal lingüístico (Base de datos terminológica) <https://www.microsoft.com/Language/es-es/Search.aspx?sString=add-on&langID=es-es> [Fecha de la consulta: 12 de octubre, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 106	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **adware**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**adware**
DEFINICIÓN Son aquellos programas que muestran publicidad utilizando cualquier tipo de medio, por ejemplo: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. Puede instalarse con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así.	

Lo mismo ocurre con el conocimiento o falta del mismo acerca de sus funciones.

FUENTE DE LA DEFINICIÓN

Glosario Técnico. Antivirus Panda.

<http://www.pandasecurity.com/spain/homeusers/security-info/glossary/>

[Fecha de la consulta: 12 de octubre, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 107	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **algorithm**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.

EQUIVALENTE **algoritmo**

DEFINICIÓN

Conjunto de procedimientos mediante los que se consigue un efecto. Suelen expresarse a través de letras, cifras y símbolos, que forman un algoritmo determinado.

Dícese del procedimiento para resolver problemas en términos de las acciones a ejecutar o el orden en que se ejecutarán dichas acciones en un problema dado.

Conjunto de Instrucciones que especifican la secuencia de operaciones a realizar, en orden, para resolver un sistema específico o clase de problema.

FUENTE DE LA DEFINICIÓN

Glosario.net - Diccionario de términos técnicos.

<http://tecnologia.glosario.net/terminos-tecnicos-internet/algoritmo-65.html>

[Fecha de la consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 108	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **attack**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**ataque**
DEFINICIÓN Un "ataque" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño. Los ataques siempre se producen en Internet, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, etc.) sin que el propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos. Para bloquear estos ataques, es importante estar familiarizado con los principales tipos y tomar medidas preventivas.	
FUENTE DE LA DEFINICIÓN CCM - High-Tech. <http://es.ccm.net/contents/17-introduccion-a-los-ataques> [Fecha de la consulta: 12 de octubre, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 3	AUTOR Y FECHA MJPM, 3 de septiembre, 2014
TÉRMINO **attachment**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**adjunto**
DEFINICIÓN Un archivo adjunto, archivo anexo, adjunto de correo o, en inglés, attachment es un	

archivo que se envía junto a un mensaje de correo electrónico. Pueden ser enviados no codificados o codificados de diferentes maneras: base64, binhex, UUEncode, quoted-printable. En MIME, el formato de correo electrónico estándar, los mensajes y sus adjuntos son mandados con el tipo multipart message, habitualmente usando base64 para adjuntos que no son texto. Los archivos adjuntos de mensajes de correo electrónico representan el método más habitual de "infectar" un equipo con un virus. En ocasiones basta con abrir el mensaje para desencadenar el virus.

FUENTE DE LA DEFINICIÓN

Microsoft Office - Portal lingüístico (Base de datos terminológica)

<http://office.microsoft.com/es-es/powerpoint-help/protejase-la-seguridad-en-office-RZ001042584.aspx?section=11>

[Fecha de consulta: 3 de septiembre, 2014]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 109	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **authentication**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.

EQUIVALENTE **autenticación**

DEFINICIÓN

Autenticación es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser). La autenticación por sí sola no verifica derechos de acceso del usuario; estos se confirman en el proceso de autorización.

FUENTE DE LA DEFINICIÓN

Escuela de Ingeniería. Comisión Interamericana de Telecomunicaciones. Organización de los Estados Americanos.

<http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: NEOLOGISMO.

FICHA Nº 4	AUTOR Y FECHA MJPM, 8 de septiembre, 2014
TÉRMINO **authorization**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**autorización**
DEFINICIÓN Una vez autenticado el usuario, los servicios de autorización determinan a qué recursos puede acceder el usuario y qué operaciones está habilitado para realizar. Un ejemplo es "El usuario 'estudiante' puede acceder al servidor host XYZ mediante Telnet únicamente".	
FUENTE DE LA DEFINICIÓN CISCO Networking Academy - Material especializado <http://cisco.infomerce.es/CCNA_RS/course/module11/11.2.3.2/11.2.3.2.html> [Fecha de consulta: 8 de septiembre, 2014]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 110	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **bastion host**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**host de bastión**
DEFINICIÓN Antes de hablar de cortafuegos es casi obligatorio dar una serie de definiciones de partes o características de funcionamiento de un firewall; por máquina o host bastión (también se denominan gates) se conoce a un sistema especialmente asegurado, pero en principio vulnerable a todo tipo de ataques por estar abierto a Internet, que tiene como función ser el punto de contacto de los usuarios de la red interna de una organización con otro tipo de redes. El host bastión filtra tráfico de entrada y salida, y también esconde la configuración de la red hacia fuera.	

FUENTE DE LA DEFINICIÓN RedIRIS. Red académica y de investigación española. <https://www.rediris.es/cert/doc/unixsec/node23.html> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 111	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **biometrics**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**biometría**
DEFINICIÓN Tecnologías que miden y analizan las características físicas y del comportamiento humano, como por ejemplo, huellas, retinas oculares e iris, patrones de voz, patrones faciales, medida de la mano, patrones de escritura y firma para reconocer o autenticar la identidad.	
FUENTE DE LA DEFINICIÓN Microsoft Office - Portal lingüístico (Base de datos terminológica) <https://www.microsoft.com/Language/es-es/Search.aspx?sString=add-on&langID=es-es> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 112	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **biometrics devices**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.

EQUIVALENTE	**dispositivos biométricos**

DEFINICIÓN

Un sistema biométrico en general consta de componentes tanto hardware como software necesarios para el proceso de reconocimiento. Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes:

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autentificación de la voz
- Reconocimiento de la firma

FUENTE DE LA DEFINICIÓN

Sistemas Biométricos - Universidad de Castilla la Mancha.

<https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: NEOLOGISMOS.

FICHA Nº 6	**AUTOR Y FECHA** **MJPM, 11 de septiembre, 2014**
TÉRMINO **bit**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.

EQUIVALENTE	**bit**

DEFINICIÓN

El bit es la unidad mínima del código binario usado por los ordenadores para almacenar información. El código binario es el lenguaje usado por los ordenadores, y

consiste de largas sucesiones de bits, pudiendo tener cada bit dos posibles valores, 0 y 1, de ahí el nombre de sistema binario. En realidad el código binario sigue las mismas pautas que nuestro código decimal, pero en vez de tener 10 posibles valores para cada posición, solo tiene dos.

FUENTE DE LA DEFINICIÓN

Mastermagazine - Revista especializada

<http://www.mastermagazine.info/termino/4050.php>

[Fecha de consulta: 11 de septiembre, 2014]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 114	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **bot**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.

EQUIVALENTE **bot**

DEFINICIÓN

Como definición general, un bot es cualquier software automatizado para ejecutar tareas específicas sin supervisión. Específicamente tenemos tres areas de aplicación más frecuentes: El bot de chat, que por ejemplo puede saludar a toda persona que entra al chat y tratar de animarlos a que tomen parte en la discusión; el bot que ejecuta búsquedas y actualizaciones en páginas web para informar al usuario cuando alguna página está cambiada; y los bots en juegos, especialmente juegos en línea, que son enemigos controlados por el computador y que toman la parte de oponentes para animar al jugador antes de que alguna presa más interesante (como tu amigo) haga su apariencia.

FUENTE DE LA DEFINICIÓN

Glosario.net - Diccionario de términos técnicos.

<http://tecnologia.glosario.net/terminos-tecnicos-internet/bot-%28robot%29-210.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 7	AUTOR Y FECHA MJPM, 11 de septiembre, 2014
TÉRMINO **BPN**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**BPN**
DEFINICIÓN *Business Process Management*, Se puede definir a BPM como una disciplina o enfoque disciplinado orientado a los procesos de negocio, pero realizando un enfoque integral entre procesos, personas y tecnologías de la información. BPM busca identificar, diseñar, ejecutar, documentar, monitorear, controlar y medir los procesos de negocios que una organización implementa. El enfoque contempla tanto procesos manuales como automatizados y no se orienta a una implementación de software. Algo importante a tener presente es que BPM no es una tecnología de software, pero se apoya y hace uso de las mismas para su implementación efectiva. Dependiendo del uso del enfoque y su aplicación, BPM puede verse como una metodología, como una herramienta estratégica o bien como conjunto de herramientas tecnológicas, no existe definición precisa, todo depende del prisma que utilicemos para ver la realidad. No obstante, personalmente creo que la definición de "enfoque disciplinado" es el mejor acercamiento para describirla.	
FUENTE DE LA DEFINICIÓN IBM Developer Works® <http://www.ibm.com/developerworks/ssa/local/websphere/introduccion-bpm/> [Fecha de consulta: 11 de septiembre, 2014]	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 8	AUTOR Y FECHA MJPM, 11 de septiembre, 2014
TÉRMINO **broadcast**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**transmisión**

DEFINICIÓN

Uno de los principales puntos de estudio de la Informática es justamente el de la Tasa de Bits, siendo principalmente conocida como la Velocidad de Transferencia, que es básicamente la rapidez con la que se pueden comunicar dos dispositivos digitales mediante un sistema dado de transmisión de datos.

La Velocidad de Transferencia entonces se desglosa en dos conceptos fundamentales:

* Tasa de Bits Constante (CBR): La cantidad de datos enviados es uniforme, por lo que no se tienen en cuenta los factores anteriormente mencionados, ni la densidad de información que es enviada en uno u otro momento
* Tasa de Bits Variable (VBR): En este caso, la medición no es uniforme sino que se realiza una diferencia entre las zonas de menor o mayor densidad, siendo entonces una cantidad mucho más precisa.

FUENTE DE LA DEFINICIÓN

Mastermagazine - Revista especializada

<http://www.mastermagazine.info/termino/4050.php>

[Fecha de consulta: 11 de septiembre, 2014]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 9	**AUTOR Y FECHA** **MJPM, 11 de septiembre, 2014**
TÉRMINO **buffer**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.

EQUIVALENTE **búfer**

DEFINICIÓN

El concepto de buffer, o búfer como le llaman algunos en español, está muy ligado a lo que sería su traducción literal: amortiguación o zona de amortiguación. De hecho, la mejor forma de explicar cómo funciona se basa en usar un símil automovilístico: los amortiguadores funcionan recibiendo el impacto directo de los vaivenes del coche, y lo regulan, dejándolo salir no de golpe, sino de forma suave, de modo que para el usuario el impacto final es mínimo y el confort máximo.

FUENTE DE LA DEFINICIÓN

Mastermagazine - Revista especializada

<http://www.mastermagazine.info/termino/4106.php>

[Fecha de consulta: 11 de septiembre, 2014]
OBSERVACIONES: NEOLOGISMOS.

FICHA Nº 10	**AUTOR Y FECHA** **MJPM, 11 de septiembre, 2014**
TÉRMINO **buffer overflow**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**desbordamiento de búfer**
DEFINICIÓN Ataque de desbordamiento de búfer: Tipo de ataque DoS (*Denial of Service*, Dengación de servicio) que se producen cuando se colocan en el búfer más datos de los que puede admitir, desbordándolo (como su nombre implica).	
FUENTE DE LA DEFINICIÓN Windows XP Service Pack 2 (parte 7): Protección contra desbordamientos de búfer <http://support.microsoft.com/kb/889741/es> [Fecha de consulta: 11 de septiembre, 2014]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 115	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **CCTV**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**CCTV**
DEFINICIÓN Closed-Circuit Televisión, Televisión de circuito cerrado: Cámara de vigilancia utiliza para la monitorización del acceso físico.	
FUENTE DE LA DEFINICIÓN	

Glosario. Seguridad Informática. CompTIA Security+ (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 116	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **CHAP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**CHAP**
DEFINICIÓN CHAP (Challenge Handshake Authentication Protocol, Protocolo de autenticación por desafío mutuo): Protocolo que desafía a un sistema para verificar la identidad. CHAP es una mejora de PAP (Password Authentication Protocol, Protocolo de autenticación de contraseña) en el que se incorpora un algoritmo hash simple a un desafío de tres vías. RFC 1334 se aplica tanto a PAP como a CHAP.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 11	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **CIA**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**CIA**
DEFINICIÓN *Confidentiality, integrity and availability*. Confidencialidad: Certeza de que los datos siguen siendo privados y nadie puede verlos excepto los que se espera que lo hagan. Integridad de datos: Cualidad que proporciona un nivel de seguridad de que los datos no se han puesto en peligro y siguen siendo secretos. Disponibilidad: La habilidad de	

un recurso para que se pueda acceder a él, se suele expresar mediante un período temporal. Muchas redes limitan la habilidad de los usuarios para acceder a los recursos de la red a sus horas de trabajo, como precaución de seguridad.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 117	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **client**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**cliente**
DEFINICIÓN Un ordenador o una aplicación que recurre a los servicios de un servidor. (modelo cliente-servidor) Es una manera muy utilizada de escribir el paradigma de diversos protocolos de red.	
FUENTE DE LA DEFINICIÓN *Glosario.net - Diccionario de términos técnicos.* <http://tecnologia.glosario.net/terminos-tecnicos-internet/client-server-model-327.html> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 12	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **common access card**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**tarjeta de acceso común**

DEFINICIÓN **CAC (*Common Access Card*, Tarjeta de acceso común):** Tarjeta de identificación estándar utilizada por el Departamento de Defensa y otros empleados. Se utiliza para la autenticación y la identificación.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 13	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **cookie**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**cookie**
DEFINICIÓN Archivo de texto simple almacenado en su máquina que contiene información sobre usted (y sus preferencias) y puede utilizarlo el servidor.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 14	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **cross-site scripting**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**filtro de scripts de sitios**
DEFINICIÓN Los scripts entre sitios (XSS) son una vulnerabilidad de seguridad de sistemas	

que generalmente se encuentra en las aplicaciones web. Permite a los usuarios malintencionados esquivar los mecanismos de seguridad del lado del cliente, que imponen los navegadores web modernos en el contenido web, inyectando scripts maliciosos en las páginas web que visualizan otros usuarios.

XSS puede suponer un riesgo de seguridad significativo dependiendo de la confidencialidad de los datos. En versiones de IBM® SPSS Collaboration and Deployment Services anteriores a la 5.0.0.0, se disponía de un filtro de seguridad web que ayudaba a impedir ataques XSS mediante la validación de los parámetros especificados por los usuarios. Sin embargo, todos los criterios de filtrado estaban empotrados en el producto de forma que los usuarios no podían editarlos ni personalizarlos. Con IBM SPSS Collaboration and Deployment Services Deployment Manager, los usuarios pueden ahora añadir, modificar y suprimir las reglas de filtro de XSS en función de la política de seguridad de su empresa.

FUENTE DE LA DEFINICIÓN

IBM Knowledge Center

<http://www.ibm.com/support/knowledgecenter/es/SS69YH_7.0.0/cads_admin_common_ddita/model_management/thick/admin_xss.html>

[Fecha de consulta: 13 de agosto, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 15	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **DAC**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**DAC**

DEFINICIÓN

Discretionary Access Control, Control de acceso discrecional. Método para restringir el acceso a los objetos basándose en la identidad de los sujetos o grupos a los que pertenecen.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 16	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **datagram**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**datagrama**
DEFINICIÓN Descriptor de paquete UDP (*User Datagram Protocol*, Protocolo de datagrama de usuario) de la capa 3 del modelo OSI.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 17	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **digital**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**digital**
DEFINICIÓN El término digital se usa comúnmente para referirse a todos aquellos sistemas que representan, almacenan o usan la información en sistema binario, esto es, a casi todos los aparatos electrónicos e informáticos que nos rodean actualmente. También se usa frecuentemente el término digital para aquellos aparatos que transmiten la información por medios de números (dígitos). Así, un reloj podría ser digital, del mismo modo que una calculadora... etc. De cualquier modo, el uso más extendido del término es el primero,	

equiparando los sistemas que usen códigos digitales (con dígitos) a los sistemas digitales. El código digital más extendido es el binario, que usan casi todos los ordenadores y que otorga dos posibles valores (uno y cero) a cada unidad de información, construyéndose ésta a través de enormes cadenas lineales de ceros y unos. Del mismo modo, nuestro sistema numérico es también un sistema digital, puesto que usa dígitos del 0 al 9. No es frecuente, pero algunas máquinas se pueden basar en él.

FUENTE DE LA DEFINICIÓN

*Master Magazine** - Revista especializada

<http://www.mastermagazine.info/termino/4618.php>

[Fecha de consulta: 13 de agosto, 2016]

OBSERVACIONES: NEOLOGISMOS.

* Master Magazine - Revista especializada en la que escriben expertos del sector y explican los términos más novedosos del sector. En el caso de las nuevas tecnologías a veces resulta imposible recurrir a diccionarios, ya que la información que ofrecen no está actualizada. La seguridad informática está en constante evolución y los términos aparecen y evolucionan de forma muy rápida, por lo que hay que recurrir a los propios expertos del sector para documentarse.

FICHA Nº 118	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **DMZ**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**DMZ**

DEFINICIÓN

DMZ (Demilitarizaed Zone, Zona desmilitarizada): Área para colocar servidores Web u otros fuera del cortafuegos, aislándolo del acceso de red interno.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 18	AUTOR Y FECHA MJPM, 13 de agosto, 2016
TÉRMINO **DNS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**DNS**
DEFINICIÓN DNS inverso: Utilizar una dirección IP para encontrar un nombre de dominio en lugar de emplear el nombre de dominio para encontrar una dirección IP (DNS normal). Los registros PTR se utilizan para las búsquedas inversas y el DNS inverso suele usarse para autenticar conexiones entrantes.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 119	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **DSSS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**DSSS**
DEFINICIÓN DSSS (Direct-Sequence Spread Spectrum, Espectro ensanchado por secuencia directa): Tecnología de comunicación que se utiliza para la comunicación en el estándar 802.11.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 120	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **EMI**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**EMI**
DEFINICIÓN EMI (Electromagnetic Interference, Interferencia electromagnética): Interferencia que se produce durante las transmisiones sobre cable de cobre debido a la energía electromagnética fuera del cable. El resultado es la degradación de la señal.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 121	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **encryption**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**cifrado**
DEFINICIÓN (cifrado, encriptación) Se trata de un mecanismo de seguridad en Internet cuya principal función es la de hacer llegar la información a un determinado usuario sin que nadie más pueda tener acceso a ella. Existen diversos tipos de cifrados que en cierta manera son la base de la seguridad de la red.	
FUENTE DE LA DEFINICIÓN *Glosario.net - Diccionario de términos técnicos.* <http://tecnologia.glosario.net/terminos-tecnicos-internet/encryption-626.html> [Fecha de consulta: 12 de octubre de 2016]	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 19	AUTOR Y FECHA MJPM, 13 de agosto, 2016
TÉRMINO **Ethernet**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**Ethernet**

DEFINICIÓN

Ethernet (también conocido como estándar IEEE 802.3) es un estándar de transmisión de datos para redes de área local que se basa en el siguiente principio:
Todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos.

Se distinguen diferentes variantes de tecnología Ethernet según el tipo y el diámetro de los cables utilizados:

* 10Base2: el cable que se usa es un cable coaxial delgado, llamado thin Ethernet.
* 10Base5: el cable que se usa es un cable coaxial grueso, llamado thick Ethernet.
* 10Base-T: se utilizan dos cables trenzados (la T significa twisted pair) y alcanza una velocidad de 10 Mbps.
* 100Base-FX: permite alcanzar una velocidad de 100 Mbps al usar una fibra óptica multimodo (la F es por Fiber).
* 100Base-TX: es similar al 10Base-T pero con una velocidad 10 veces mayor (100 Mbps).
* 1000Base-T: utiliza dos pares de cables trenzados de categoría 5 y permite una velocidad de 1 gigabite por segundo.
* 1000Base-SX: se basa en fibra óptica multimodo y utiliza una longitud de onda corta (la S es por short) de 850 nanómetros (770 a 860 nm).
* 1000Base-LX: se basa en fibra óptica multimodo y utiliza una longitud de onda larga (la L es por long) de 1350 nanómetros (1270 a 1355 nm).

Todos los equipos de una red Ethernet están conectados a la misma línea de transmisión y la comunicación se lleva a cabo por medio de la utilización un protocolo denominado CSMA/CD (Carrier Sense Multiple Access with Collision Detect que significa que es un protocolo de acceso múltiple que monitorea la portadora: detección de portadora y detección de colisiones).

FUENTE DE LA DEFINICIÓN

Enciclopedia › Redes › Tecnologías de Internet

<http://es.ccm.net/contents/672-ethernet>

[Fecha de consulta: 13 de agosto, 2016]
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 122	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **Extranet**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**Extranet**
DEFINICIÓN Servicios Web o similares establecidos en una red privada para que entidades externas seleccionadas, por ejemplo, fabricantes y proveedores, accedan a ellos de forma interna.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 20	**AUTOR Y FECHA** **MJPM, 13 de agosto, 2016**
TÉRMINO **extrusion**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**extrusión**
DEFINICIÓN Examinar los datos que salen de una red para detectar signos de tráfico malicioso.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 123	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **FHSS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**FHSS**
DEFINICIÓN FHSS (Frequency-Hopping Spread Spectrum, Espectro ensanchado por salto de frecuencia): Tecnología de comunicación utilizada para comunicarse en el estándar 802.11. FHSS consigue la comunicación a través de saltos de transmisión en un rango de frecuencias predefinidas.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 124	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **firewall**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**cortafuegos**
DEFINICIÓN Combinación de hardware y software que protege una red frente a ataques realizados por piratas informáticos que podrían acceder a través de redes públicas, incluyendo Internet.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 21	AUTOR Y FECHA MJPM, 13 de agosto, 2016
TÉRMINO **FTP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**FTP**
DEFINICIÓN *File Transfer Protocol*, Protocolo para la transferencia de archivos. TCP/IP y software que permiten transferir archivos entre sistemas informáticos y utilizar contraseñas de texto simple. Debido a que FTP se ha implementado en muchos tipos de sistemas informáticos, los archivos pueden transferirse entre sistemas dispares (por ejemplo, un ordenador personal y un miniordenador). Véase también TCP/IP.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 22	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **FTPS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**FTPS**
DEFINICIÓN Conocido preferentemente por sus siglas de FTP (en inglés, File Transfer Protocol) este protocolo de red llamado Protocolo de Transferencia de Archivos es como su nombre lo indica una de las formas en la cual podemos enviar archivos hacia una Red TCP (siglas en inglés de Transmission Control Protocol) en la que utilizaremos la clásica arquitectura de Cliente - Servidor para dicha transferencia. De este modo, tenemos desde nuestro ordenador que oficiará como Cliente la posibilidad de poder establecer un vínculo con un Servidor remoto para poder o bien descargar archivos desde esta dirección de destino, o bien poder cargar archivos mediante un envío del mismo, sin tener en cuenta como condicionante al Sistema Operativo que se esté utilizando en	

cada extremo de la comunicación de datos.

FUENTE DE LA DEFINICIÓN

*Master Magazine** - Revista especializada

<http://www.mastermagazine.info/termino/5086.php>

[Fecha de consulta: 15 de agosto, 2016]

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

* Master Magazine - Revista especializada en la que escriben expertos del sector y explican los términos más novedosos del sector. En el caso de las nuevas tecnologías a veces resulta imposible recurrir a diccionarios, ya que la información que ofrecen no está actualizada. La seguridad informática está en constante evolución y los términos aparecen y evolucionan de forma muy rápida, por lo que hay que recurrir a los propios expertos del sector para documentarse.

FICHA Nº 23	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **gateway**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**puerta de enlace**

DEFINICIÓN

Con el objetivo de acceder a una red exterior desde una red local (LAN), se configuran puertas de enlace o Gateways, los cuales son normalmente equipos de computación preparados para tal fin. De este modo se conectam mediante protocolos y arquitecturas disímiles, diversas redes informáticas formadas por todo tipo de hardware y software.

Las operaciones realizadas por el gateway para brindar acceso a una red externa tienen que ver en su mayoría con Network Address Translation (NAT), traducciones de direcciones de red.

De este modo el enmascaramiento de IP, o IP Masquerading es la técnica que se emplea normalmente para dar acceso a la red de redes a las computadoras de la red local, compartiendo una misma IP externa proveniente de la misma conexión a Internet.

FUENTE DE LA DEFINICIÓN

*Master Magazine** - Revista especializada

<http://www.mastermagazine.info/termino/5120.php>

[Fecha de consulta: 15 de agosto, 2016]

OBSERVACIONES: NEOLOGISMOS.

* *Master Magazine* - Revista especializada en la que escriben expertos del sector y explican los términos más novedosos del sector. En el caso de las nuevas tecnolgías a veces resulta imposible recurrir a diccionarios, ya que la información que ofrecen no está actualizada. La seguridad informática está en constante evolución y los términos aparecen y evolucionan de forma muy rápida, por lo que hay que recurrir a los propios expertos del sector para documentarse.

FICHA Nº 125	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **hacker**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**hacker**
DEFINICIÓN En general, se utiliza para hacer referencia a alguien que obtiene acceso a un sistema, software o hardware sin permiso. También se conoce como cracker.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 24	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **honeynet**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**honeynet**

DEFINICIÓN

Una Honeynet tiene como objetivo reunir información sobre la actividad del intruso. De esta manera seremos capaces de detectar una vulnerabilidad antes de que sea explotada, además de conocer los riesgos a los cuales nuestros sistemas de producción están expuestos. Una de las ventajas de las Honeynets es que nos proveen de la inteligencia necesaria para conocer los riesgos con los cuales contamos en la red, además de poner de nuestro lado la capacidad de implantar seguridad proactiva, siendo esto último un punto crucial en la defensa de toda organización. Desde los inicios de la milicia, se ha sabido que si no se cuenta con la capacidad ofensiva para enfrentar al enemigo, no se podrá ganar alguna guerra. Desde la óptica de seguridad en redes, esta es una de las ideas principales en el que se centra el concepto de una Honeynet, aprender cuanto sea posible de las amenazas y del comportamiento de los atacantes, para implantar una arquitectura de seguridad proactiva que nos permita no solo defendernos de tales amenazas, si no también someterlas antes de que sucedan.

FUENTE DE LA DEFINICIÓN

"Coordinación de Seguridad de la Información - Introducción a las Honeynets"
<http://www.asc.unam.mx/descarga.dsc?arch=247>
[Fecha de consulta: 15 de agosto, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 126	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **honeypot**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**honeypot**

DEFINICIÓN

Sistema falso que se establece para atraer y disminuir el ritmo de un hacker. También puede emplearse para aprender sobre las técnicas y métodos de la piratería informática.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 127	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **host**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**host**
DEFINICIÓN Host: Cualquier dispositivo de red con una dirección TCP/IP. Host a host: Describe una comunicación que se producen entre host. Host de doble alojamiento: Host que reside en más de una red y tiene más de una tarjeta de red física. Host de filtrado: Enrutador que está frente a un servidor en la red privada. En general, el servidor realiza el filtrado de paquetes antes de alcanzar el cortafuegos o el servidor proxy que atiende a la red interna.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 25	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **HTTP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**HTTP**
DEFINICIÓN *Hypertext Transfer Protocol*, Protocolo de transferencia de hipertexto. Protocolo utilizado para la comunicación entre un servidor y un navegador Web.	

FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 26	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **HTTPS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**HTTPS**
DEFINICIÓN Hypertext Transfer Protocol Secure (o HTTPS) es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW, generalmente para transacciones de pagos o cada vez que se intercambie información sensible (por ejemplo, claves) en internet. De esta manera la información sensible, en el caso de ser interceptada por un ajeno, estará cifrada. El nivel de protección que ofrece depende de la corrección de la implementación del navegador web, del software y de los algoritmos criptográficos soportados. Además HTTPS es vulnerable cuando es aplicado a contenido estático públicamente disponible. El HTTPS fue creado por Netscape Communications en 1994 para su navegador Netscape Navigator.	
FUENTE DE LA DEFINICIÓN *Diccionario de informática y tecnología.* <http://www.alegsa.com.ar/Dic/https.php> [Fecha de consulta: 15 de agosto, 2016]	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 27	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **hub**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**concentrador**
DEFINICIÓN El hub (concentrador) es el dispositivo de conexión más básico. Es utilizado en redes locales con un número muy limitado de máquinas. No es más que una toma múltiple RJ45 que amplifica la señal de la red (base 10/100). En este caso, una solicitud destinada a una determinada PC de la red será enviada a todas las PC de la red. Esto reduce de manera considerable el ancho de banda y ocasiona problemas de escucha en la red. Los hubs trabajan en la primera capa del modelo OSI: <http://www.zator.com/Hardware/H12_2.htm>	
FUENTE DE LA DEFINICIÓN *CCN Enciclopedia* <http://es.ccm.net/faq/656-redes-concentrador-hub-conmutador-switch-y-router#1-el-hub> [Fecha de consulta: 15 de agosto, 2016]	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 128	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **HVAC**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**HVAC**
DEFINICIÓN Acrónimo utilizado para calefacción, ventilación y aire acondicionado. (Heating, Ventilation, and Air Conditioning, Calefacción, ventilación y aire acondicionado)	

FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 28	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **IANA**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IANA**
DEFINICIÓN *Internet Assigned Numbers Authority*, Agencia de Asignación de Números de Internet. Organización responsable de regular las direcciones IP. http://www.iana.org.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 29	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **ICMP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**ICMP**
DEFINICIÓN *Internet Control Message Protocol*, Protocolo de Mensajes de Control de Internet. Protocolo de mensajería y administración para TCP/IP. La utilidad Ping utiliza ICMP. Consulte también Ping, TCP/IP.	
FUENTE DE LA DEFINICIÓN	

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 30	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **identification**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**identificación**
DEFINICIÓN Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación. Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas: Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc. Algo que la persona posee: por ejemplo una tarjeta magnética. Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz. Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.	
FUENTE DE LA DEFINICIÓN "Seguridad de la Información: Seguridad Lógica - Identificación y Autentificación" <http://www.segu-info.com.ar/logica/identificacion.htm> [Fecha de consulta: 15 de agosto, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 129	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **IDS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IDS**
DEFINICIÓN IDS (Intrusion Detection System, Sistema para la detección de intrusiones): Herramientas que identifican y responden a ataques utilizando reglas o lógica definidas. Un IDS puede estar basado en red o en host.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 130	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **IEEE 802.11x**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IEEE 802.11x**
DEFINICIÓN La familia de protocolos IEEE 802.11x proporciona comunicaciones inalámbricas utilizando transmisiones de frecuencia de radio. Las frecuencias que emplean los estándares 802.11 son el espectro de 2.4GHz y 5GHz. Se han definido anchos de banda para entornos inalámbricos y, a excepción de 802.11a, suelen ser compatibles entre sí.	
FUENTE DE LA DEFINICIÓN Capítulo 12. *"Seguridad de red inalámbrica". Seguridad informática CompTIA Segurity+.* Guía de seguridad y certificación del examen SYO-301. 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 31	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **implicit deny**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**denegación implícita**
DEFINICIÓN Una denegación implícita significa que se deniega el usuario que no tiene un permiso explícito. Descripción del filtrado de tráfico * Las ACL están compuestas de sentencias. * Al menos una sentencia debe ser una sentencia de permiso, sino todo el tráfico será denegado. * La sentencia final es una denegación implícita. * La ACL debe aplicarse a una interfaz para que funcione.	
FUENTE DE LA DEFINICIÓN "Windows Server 2008: Administración - Preparación a la certificación MCITP" <https://books.google.es/books?id=8gKBc0RP07UC&pg=PA340&lpg=PA340&dq=%22denegaci%C3%B3n+impl%C3%ADcita%22+acl&source=bl&ots=vetlWXxdMz&sig=TekwYap6lqJsYJygAOp8xLGKodU&hl=es-419&sa=X&ved=0ahUKEwiC8KW8qcPOAhWLcRQKHUABDGcQ6AEIRTAH#v=onepage&q=%22denegaci%C3%B3n%20impl%C3%ADcita%22%20acl&f=false> [Fecha de consulta: 15 de agosto, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 131	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **Internet**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**Internet**
DEFINICIÓN Internet se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. Pero sería un error considerar Internet únicamente como una red de computadoras. Podemos considerar las computadoras simplemente como el	

medio que transporta la información. En este caso Internet sería una gran fuente de información práctica y divertida. Con Internet podemos enviar mensajes, programas ejecutables, ficheros de texto, consultar catálogos de bibliotecas, pedir libros, hacer compras, etc.
FUENTE DE LA DEFINICIÓN Universitat Jaume I - CONCEPTOS BÁSICOS SOBRE INTERNET <http://www3.uji.es/~pacheco/INTERN~1.html> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 32	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **Intranet**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**Intranet**
DEFINICIÓN Servicios Web (o similares) que es establecen en una red privada a los que solo se puede acceder de forma interna.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 33	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **IP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IP**
DEFINICIÓN	

Internet Protocol, Protocolo de Internet. En el entorno TCP/IP, protocolo responsable del direccionamiento de red. Véase también TCP/IP.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 34	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **IPS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IPS**
DEFINICIÓN IPS basado en host. HIPS (*Host-Based IPS*, Sistema de detección de intrusión basado en IPS): Sistema de detección de intrusiones basado en host. Para evitar la intrusión, primero debe detectarla (convirtiéndose en un subconjunto de HIDS) y actuar en consecuencia.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 132	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **IPSec**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IPSec**
DEFINICIÓN IPSec (IP Security, Seguridad IP): Conjunto de protocolos que habilita el cifrado, la autenticación y la integridad sobre IP. IPSec se suele utilizar con VPN (Virtual Private Networks, Redes privadas virtuales) y funciona en la	

Capa 3.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 35	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **IPv4**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IPv4**

DEFINICIÓN

IPv4 es la versión 4 del protocolo IP (Internet Protocol). Es el estándar actual de Internet para identificar dispositivos conectados a esta red.

Es uno de los protocolos más importantes para el funcionamiento de internet y fue implementado en ARPANET en 1983.

Es el protocolo que más enruta datos en internet en la actualidad, a pesar de que ya se ha lanzado hace unos años (2006) su sucesor, la versión IPv6. Ambos conviven en internet.

La estructura y funcionamiento de IPv4 está descrito en la publicación RFC 791 (septiembre de 1981) de la IETF, en reemplazo de la definición anterior (RFC 760 de enero 1980).

IPv4 utiliza direcciones IP de 32 bits (4 bytes), lo cual limita la cantidad de direcciones a 4.294.967.296 (2 elevado a 32). Esto crea un evidente problema, la escasez de direcciones. Cada dispositivo que se conecta a internet debe tener una dirección IP para ser identificado y 4 mil direcciones IP diferentes no son suficientes. Por lo que se lanzó la versión 6 (IPv6) que permite muchísimas más direcciones, comenzando su despliegue en 2006.

La cantidad de direcciones IPv4 se terminaron el 3 de febrero de 2011, luego de haber sido esto retrasado empleando varios métodos como Classful network, CIDR y NAT.

IPv4 reserva bloques de direcciones especiales para redes privadas (aproximadamente 18 millones de direcciones) y direcciones de multidifusión (aproximadamente 270 millones de direcciones).

FUENTE DE LA DEFINICIÓN

ALEGSA - Diccionario de informática y tecnología.

<http://www.alegsa.com.ar/Dic/ipv4.php>

[Fecha de consulta: 15 de agosto, 2016]

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 36	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **IPv6**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IPv6**
DEFINICIÓN Versión 6 del protocolo de internet (IP). Es un protocolo encargado de dirigir los paquetes a través de una red, especialmente Internet. Fue diseñado por Steve Deering de Xerox PARC y Craig Mudge. IPv6 fue diseñada para sustituir la versión actual (IPv4) que tiene grandes limitaciones, especialmente un limitado número de direcciones de red posibles. IPv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2 elevado a 128) de direcciones, mientras que IPv4 solo 4.294.967.296 (2 elevado a 32). El uso de IPv6 ha sido frenado temporalmente por el uso de la traducción de direcciones de red (NAT), que alivia parcialmente el problema del faltante de direcciones IP. El problema es que NAT hace difícil o imposible el uso de voz sobre IP (VoIP), los juegos multiusuarios y las aplicaciones P2P. Se estima que IPv4 seguirá funcionando hasta 2025, por la falta de renovación de dispositivos que solo funcionan con este protocolo. Un ejemplo de una dirección IP en versión 6 es: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334	
FUENTE DE LA DEFINICIÓN *ALEGSA - Diccionario de informática y tecnología.* <http://www.alegsa.com.ar/Dic/ipv6.php> [Fecha de consulta: 15 de agosto de 2016]	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 37	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam*

IPX	*SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**IPX**
DEFINICIÓN Internet Packet Exchange - Intercambio de Paquetes interred. Protocolo para el intercambio de paquetes entre aplicaciones dentro de una red Netware. Actualmente este protocolo está en desuso y solo se utiliza para juegos en red antiguos.	
FUENTE DE LA DEFINICIÓN *ALEGSA - Diccionario de informática y tecnología.* <http://www.alegsa.com.ar/Dic/ipx.php> [Fecha de consulta: 15 de agosto, 2016]	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 38	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **ISDN**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**ISDN**
DEFINICIÓN *Integrated Services Digital Network*, Red digital de servicios integrados. Estándar de telecomunicaciones que se utiliza para enviar de forma digital voz, datos y señales de vídeo por las mismas líneas.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 104	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **ISO**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**ISO**
DEFINICIÓN *International Telecomunications for Standarization*, Organización internacional de normalización. Organización de estándares que desarrollan el modelo OSI (*Open Systems Interconnection*, Interconexión de sistemas abiertos). Este modelo proporciona una directriz sobre cómo se producen las comunicaciones entre ordenadores.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 39	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **ISP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**ISP**
DEFINICIÓN *Internet Service Provider*, Proveedor de servicio de Internet. Compañía que proporciona acceso directo a Internet para los usuarios de ordenadores domésticos y empresariales.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 134	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **Kerberos**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**Kerberos**
DEFINICIÓN Esquema de autenticación que utiliza tickets (claves únicas) incrustadas en los mensajes. Recibe su nombre del mítico perro de tres cabezas que guardaba las puertas del inframundo. TACACS (Terminal Access Controller Access Control System, Sistema de control de acceso mediante control del acceso desde terminales): Sistema de autenticación que permite que acepten credenciales procedentes de varios métodos, incluyendo Kerberos. El proceso cliente/servidor TACACS se produce del mismo modo que el proceso RADIUS (Remote Authentication Dial In User Service, Servicio de autenticación remota telefónica de usuario).	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 40	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **L2TP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**L2TP**
DEFINICIÓN *Layer 2 Tunneling Protocol*, Protocolo de túnel de capa dos. Protocolo de túnel que añade funcionalidad a PPP (*Point-to-Point Protocol*, Protocolo punto a punto). Lo crearon Cisco y Microsoft y se suele utilizar con las VPN *(Virtual Private networks*, Redes privadas virtuales).	
FUENTE DE LA DEFINICIÓN	

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 41	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **LAN**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**LAN**
DEFINICIÓN *Local Area Network*, Red de área local. Red restringida a un único edificio, grupo de ellos o incluso a una sola habitación. Una red LAN puede tener uno o más servidores.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 42	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **LDAP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**LDAP**
DEFINICIÓN Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorio. Conjunto de protocolos que deriva de X.500 y opera en el puerto 389.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 43	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **link**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**enlace**

DEFINICIÓN

Enlace creado que utiliza un conmutador para limitar el tráfico de red. Un enlace en informática es una expresión que conecta una cierta información con otra. Aunque sea un concepto muy sencillo, lo cierto es que hay cientos de enlaces distintos. El enlace puede ser una imagen, una palabra, un hipertexto, una dirección web, una línea de programación, una referencia directa... que te redirige a otra información relacionada. Y al pinchar sobre el enlace se desencadena una acción que dependerá del tipo de este. Así, el enlace puede ser de ayuda, o bien redirigirte a otra página web, lanzar una aplicación, descargar un archivo, ejecutar una acción... etc.

FUENTE DE LA DEFINICIÓN

*Master Magazine** - Revista especializada.

<http://www.mastermagazine.info/termino/4888.php>

[Fecha de consulta: 15 de agosto de 2016]

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

* *Master Magazine* - Revista especializada en la que escriben expertos del sector y explican los términos más novedosos del sector. En el caso de las nuevas tecnologías a veces resulta imposible recurrir a diccionarios, ya que la información que ofrecen no está actualizada. La seguridad informática está en constante evolución y los términos aparecen y evolucionan de forma muy rápida, por lo que hay que recurrir a los propios expertos del sector para documentarse.

FICHA Nº 44	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **load balancers**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**balanceo de carga**
DEFINICIÓN Balanceo de Carga significa dividir el total de trabajo que un sistema o computadora tiene que hacer entre dos o más sistemas o computadoras. Así pues esta división de carga permite realizar el mismo trabajo en una porción de tiempo más reducida, o lo que es lo mismo; permite realizar más carga de trabajo en el mismo tiempo total. Existen numerosas formas de hacer balanceo de carga, por hardware (DNS), por software o una combinación de los dos. El balanceo de carga está especialmente indicado para entornos en los que es muy difícil prever el volumen de carga de trabajo. El factor de división de carga se puede definir, dando más o menos carga a cada uno de los sistemas implicados. Esta característica se llama carga asimétrica.	
FUENTE DE LA DEFINICIÓN "Introducción al Balanceo de Carga en Aplicaciones Web" <https://redesocialespaldava.files.wordpress.com/2012/11/articulo.pdf> [Fecha de consulta: 15 de agosto, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 45	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **login**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**login**
DEFINICIÓN 1. El login es nombre dado al momento de autentificación al ingresar a un	

servicio o sistema.

En el momento que se inicia el login, el usuario entra en una sesión, empleando usualmente un nombre de usuario y contraseña.

Por ejemplo, cuando un foro de internet pide el "login", es porque está pidiendo el nombre de usuario y contraseña que elegiste cuando te registraste en dicho foro de internet.

Suele usarse como verbo y conjugarse al españolizarse, por ejemplo: "loguearse". En inglés la acción de "loguearse" es "logging in".

Un término más apropiado para "loguearse" sería "Iniciar sesión" o "Autentificarse". La acción contraria es cerrar sesión o desidentificarse (logging out).

2. Login name, nombre de usuario. Es el nombre que adquiere el usuario para acceder a un determinado servicio. Ver nombre de usuario.

FUENTE DE LA DEFINICIÓN

ALEGSA - diccionario de informática y tecnología.

<http://www.alegsa.com.ar/Dic/login.php>

[Fecha de consulta: 15 de agosto, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 46	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **logon**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**logon**

DEFINICIÓN

Rutina de conexión a una red o estación remota (Ver: Remoto) mediante la utilización de un sistema de conexión a red o modem.

Remoto: La palabra se utiliza en tecnologías de la información para definir sistemas o elementos de sistemas que se encuentran físicamente separados de una unidad central. Un puente remoto es un dispositivo que hace posible la comunicación entre, por ejemplo, una LAN y una red de área amplia. El uso del término es muy frecuente: para referirse al mantenimiento de sistemas a distancia, al acceso a aplicaciones residentes (Ver: Residir) en unidades físicamente distantes, etc.; naturalmente, esto

implica la utilización de un software especializado. Algunos ejemplos del uso de esta palabra: gestión remota de los datos; acceso remoto a los archivos; acceso a periféricos remotos; monitorización remota; acceso remoto a DB2 (programa de gestión de bases de datos) en un sistema 370 de IBM, etc.

FUENTE DE LA DEFINICIÓN

Glosario.net - Diccionario de términos técnicos.

<http://tecnologia.glosario.net/terminos-tecnicos-internet/logon-1019.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 135	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **MAC**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**MAC**

DEFINICIÓN

MAC: Véase MAC (Media Access Control, Control de acceso a medios), MAC (Mandatory Access Control, Control de acceso obligatorio) y MAC (Message Authentication Code, Código de autenticación de mensaje).

MAC (Mandatory Access Control, Control de acceso obligatorio): Directiva de seguridad en la que se utilizan etiquetas para identificar la confidencialidad de los objetos. Cuando un usuario intenta acceder a un objeto, se comprueba la etiqueta para ver si debería permitirse el acceso (es decir, si el usurario está operando al mismo nivel de confidencialidad). Esta directiva es obligatoria por que las etiquetas se aplican automáticamente a todos los datos (y solo puede modificarlas una acción administrativa), al contrario que las directivas discrecionales que dejan decidir al usuario si aplicar una etiqueta.

MAC (Media Access Control, Control de acceso a medios): Subcapa de la capa Enlace de datos en el modelo OSI (Open Systems Interconnection, Interconexión de sistemas abiertos) que controla el modo en que varios dispositivos emplean el mismo canal de comunicación. Controla qué dispositivos pueden trasmitir y cuando pueden hacerlo.

MAC (Message Authentication Code, Código de autenticación de mensaje): Método frecuente para verificar la identidad. El MAC deriva del mensaje y de

una clave secreta.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 136	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **MAC address**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**dirección MAC**

DEFINICIÓN

Dirección que se asigna a una tarjeta de red o se graba en la NIC (Network Interface Card, Tarjeta de interfaz de red). Los PC utilizan las direcciones MAC para realizar el seguimiento de otros o para mantenerse separados.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 47	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **malicious add-ons**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**complementos maliciosos**

DEFINICIÓN

Se trata de una aplicación que se ejecuta automáticamente y que se activa a sí misma adoptando varias formas como, por ejemplo, applets de Java, controles ActiveX, contenido insertado, complementos, lenguajes de scripting u otros lenguajes

de programación diseñados para mejorar el correo electrónico y las páginas web.

Los scripts, gusanos y virus pueden dañar tu equipo mediante la búsqueda de puntos de entrada hacia tus datos de más valor. Visitar sitios web infectados o hacer clic en un archivo adjunto o enlace dañado de un correo electrónico constituyen las principales vías de entrada por las que los códigos maliciosos acceden a tu sistema. La mejor defensa ante estas amenazas es contar con un software antivirus que disponga de actualizaciones automáticas, soluciones de eliminación de malware, protección para navegar por la Web y la capacidad de detectar todo tipo de infecciones.

FUENTE DE LA DEFINICIÓN

© 2016 AO Kaspersky Lab. Internet Security Center

<http://www.kaspersky.es/internet-security-center/definitions/malicious-code>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 48	AUTOR Y FECHA MJPM,15 de agosto, 2016
TÉRMINO **mandatory access control**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**control de acceso obligatorio**

DEFINICIÓN

Mandatory Access Control, Control de acceso obligatorio. Directiva de seguridad en la que se utilizan etiquetas para identificar la confidencialidad de los objetos. Cuando un usuario intenta acceder a un objeto, se comprueba la etiqueta para ver si debería permitirse el acceso (es decir, si el usurario está operando al mismo nivel de confidencialidad). Esta directiva es obligatoria por que las etiquetas se aplican automáticamente a todos los datos (y solo puede modificarlas una acción administrativa), al contrario que las directivas discrecionales que dejan decidir al usuario si aplicar una etiqueta.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 137	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **mantrap**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**mantrap**
DEFINICIÓN Dispositivo, como una pequeña habitación, que limita el acceso a uno o varios individuos. Suelen utilizar candados electrónicos y otros métodos para el control de acceso.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 49	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **modem**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**módem**
DEFINICIÓN Es un elemento físico (un periférico), también conocido como MOdulador DEMmodulador, que se utiliza para convertir las señales eléctricas (analógicas y digitales). Su objetivo es facilitar la comunicación entre ordenadores y otros tipos de equipos. Su utilidad más habitual, en la actualidad, es conectar los ordenadores a Internet.	
FUENTE DE LA DEFINICIÓN *Glosario.net - Diccionario de términos técnicos.* <http://tecnologia.glosario.net/terminos-tecnicos-internet/logon-1019.html> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 50	AUTOR Y FECHA MJPM 15 de agosto, 2016
TÉRMINO **multicasting**	REFERENCIA *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**multidifusión**
DEFINICIÓN Enviar datos a más de una dirección.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 51	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **multihoming**	REFERENCIA *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**multihoming**
DEFINICIÓN El Multihoming se define como la conexión de un AS a más de un ISP a la vez. La forma más común de implementar multihoming es obtener un bloque de direcciones independientes del proveedor junto con un número de sistema autónomo (ASN) y anunciar el bloque de direcciones vía BGP a cada uno de los ISPs a los que se está conectado. Si a un sitio no le es posible hacer multihoming con direcciones independientes del proveedor aún le es posible obtener un bloque de direcciones de uno de los ISPs que le prestan servicio. El AS cliente anuncia su bloque de direcciones por BGP a todos los ISPs, los cuales a su vez lo anuncian hacia Internet. Pero el ISP que delegó el bloque, además de anunciar el bloque del AS cliente, anuncia su bloque mayor que lo engloba. De esta forma, aunque el bloque pequeño fuese filtrado en algún lugar de la red, al menos quedaría una ruta hacia el bloque que le dio origen.	

Este modelo de multihoming con direcciones asignadas por el proveedor permite gozar de buena parte de las ventajas del multihoming a sitios que no son lo suficientemente grandes como para obtener un bloque independiente del proveedor.
FUENTE DE LA DEFINICIÓN Proyectos Abreproy <http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F9.+Multihoming.pdf> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 52	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **NAC**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**NAC**
DEFINICIÓN *Network Access Control*, Control de acceso de red. Conjunto de estándares que define la red para los clientes que intenten acceder a ella. En general, NAC requiere que los clientes estén libres de virus y que se adhieran a unas políticas específicas antes de que se les permita el acceso.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 53	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **NAT**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**NAT**
DEFINICIÓN *Network Address Translation*, Traducción de direcciones de Internet.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 54	**AUTOR Y FECHA** **MJPM 15 de agosto, 2016**
TÉRMINO **NCP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**NCP**
DEFINICIÓN *Network Control Protocol*, Protocolo de control de red. El protocolo PPP (*Point-to-Point Protocol*, Protocolo punto a punto) lo emplea para encapsular el tráfico de red.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 55	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **NetBIOS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**NetBIOS**
DEFINICIÓN	

(Network BIOS. Network Basic Input/Output System). Bios de una red. Sistema Basico de Entrada/Salida de una red.
FUENTE DE LA DEFINICIÓN *Glosario.net - Diccionario de términos técnicos.* <http://tecnologia.glosario.net/terminos-tecnicos-internet/netbios-1205.html> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 138	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **network**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**red**
DEFINICIÓN Red: Grupo de dispositivos conectados a través de algunos medios con el propósito de compartir información o recursos. Red cliente/servidor: Red en la que todos los recursos se almacenan en un servidor de archivos y la energía de procesamiento se distribuye entre los terminales y el servidor de archivos. Red con resistencia a fallos: Red que funciona como mínimo el 99 por ciento de las veces o que tiene menos de 8 horas al año de interrupción. Red de área amplia: Véase WAN. Red de tolerancia a errores: Red que puede recuperarse de errores menores. Red privada: La parte de una red que está detrás del cortafuegos y no se ve en Internet. Véase también	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 56	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **network segmentation**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**segmentación de red**

DEFINICIÓN

Segmentar una red consiste en dividirla en subredes para poder aumentar el número de ordenadores conectados a ella y así aumentar el rendimiento, tomando en cuenta que existe una única topología, un mismo protocolo de comunicación y un solo entorno de trabajo.

Un segmento es un bus lineal al cual están conectadas varias estaciones. Las características son:

- Cuando se tiene una red grande se divide en trozos llamados segmentos.

- Para interconectar varios segmentos se utilizan bridges o routers.

- Al dividir una red en segmentos, aumenta su rendimiento.

- A cada segmento y a las estaciones conectadas a el se le llama subred.

Cuando se segmenta una red, se están creando subredes que se autogestionan, de forma que la comunicación entre segmentos solo se realiza cuando es necesario, mientras tanto, la subred está trabajando de forma independiente.

El dispositivo utilizado para segmentar la red debe ser inteligente, ya que debe ser capaz de decidir a qué segmento va a enviar la información que llego a el. Se pueden utilizar hubs, repetidores, bridges, routers, gateways.

La segmentación de una red se hace necesaria cuando:

- Se va a sobrepasar el número de nodos que la topología permite.

- Mejorar el tráfico de una red.

FUENTE DE LA DEFINICIÓN

TECNOLOGÍAS DE LA INFORMACIÓN - Segmentación y direccionamiento IP

<http://redes1ti.blogspot.com.es/2013/02/segmentacion-y-direccionamiento-ip.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 57	AUTOR Y FECHA MJPM 15 agosto, 2016
TÉRMINO **NIC**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**NIC**
DEFINICIÓN *Network Interface Card*, Tarjeta de interfaz de red. Dispositivo físico que conecta ordenadores y otros equipos de red a los medios de transmisión.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+ (Títulos Especiales).* 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 58	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **NIDS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**NIDS**
DEFINICIÓN *Network-Based IDS*, IDS basado en red. Enfoque de IDS (*Intrusion Detection System*, Sistema para la detección de intrusiones). Adjunta el sistema a un punto de la red en que puede monitorizar y comunicar todo el tráfico de red.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 59	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **NIPS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**NIPS**
DEFINICIÓN *Network-Based IPS*, IPS basado en red. Sistema de prevención de intrusiones que se basa en red. Para evitar la intrusión, primero debe detectarla (siendo así un subconjunto de IDS) y, a continuación, actuar en consecuencia.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 139	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **partitioning**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**particionamiento**
DEFINICIÓN Proceso de descomponer una red en componentes más pequeños que pueden protegerse de forma individual.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 60	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **password**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**contraseña**
DEFINICIÓN Las contraseñas son claves que usamos para tener acceso a nuestra información privada que se encuentra almacenada en alguna computadora, correo electrónico, cuentas bancarias o cualquier otra fuente de Almacenamiento de información, ya sea privada o confidencial. El problema principal de la seguridad radica en el empleo de contraseñas débiles para la protección de los Datos, ya que esto permite que los intrusos realicen distintos ataques contra sistemas tratando de comprometer su seguridad. La mejor solución ante ello es el empleo de contraseñas robustas que otorguen un grado de seguridad más Elevado para la protección de la información. Uno de los inconvenientes principales en el empleo de Contraseñas robustas es que son difíciles de recordar, sin embargo existen técnicas que permiten utilizarlas sin necesidad de anotarlas en algún lugar físicamente o decírselas a alguien más.	
FUENTE DE LA DEFINICIÓN "Seguridad Informatica". Trabajo realizado por: Daniela Valdovinos, Daniel Solano, Ramses Saldivar, Andre Andrade. 3c TSMEC <http://seguridadinformatica3c.blogspot.com.es/2012/10/contrasena-segura.html> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 61	AUTOR Y FECHA MJPM, 15 de agosto, 2016
TÉRMINO **PBX system**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**sistema PBX**
DEFINICIÓN	*Private Branch Exchange*, Central de conmutación privada. Sistema que permite a los usuarios conectar voz, datos, localizadores, redes y casi cualquier otra aplicación en un único sistema de comunicaciones. Un sistema PBX permite que una organización establezca su propia compañía telefónica.
FUENTE DE LA DEFINICIÓN	Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES:	TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 140	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **perimeter**	**REFERENCIA** CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301, 5th Edition. 2011.
EQUIVALENTE	**perímetro**
DEFINICIÓN	Perímetro de seguridad: Protección establecida en el exterior de una red o de un servidor para protegerlos.
FUENTE DE LA DEFINICIÓN	Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES:	TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 62	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **personal identification verification card**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**tarjeta de verificación de identificación personal**

DEFINICIÓN

Autenticación es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser). La autenticación por sí sola no verifica derechos de acceso del usuario; estos se confirman en el proceso de autorización.

En general, la seguridad de las redes de datos requiere para conceder acceso a los servicios de la red, tres procesos: (1) autenticación, (2) autorización y (3) registro.

Autenticación: el proceso por el cual el usuario se identifica en forma inequívoca; es decir, sin duda o equivocación de que es quien dice ser.

Autorización: el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

Registro: el proceso mediante el cual la red registra todos y cada uno de los accesos a los recursos que realiza el usuario, autorizado o no.

Estos tres procesos se conocen por las siglas en inglés como AAA, o Authentication, Authorization, y Accounting.

FUENTE DE LA DEFINICIÓN

Escuela de Ingeniería. Comisión Interamericana de Telecomunicaciones. Organización de los Estados Americanos.

<http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp>

[Fecha de consulta: 12 de octubre de 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 141	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **physical barriers**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**barreras físicas**

DEFINICIÓN

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial. Más claramente, y particularizando para el caso de equipos Unix y sus centros de operación, por `seguridad física' podemos entender todas aquellas mecanismos - generalmente de prevención y detección - destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

FUENTE DE LA DEFINICIÓN

RedIRIS. Red académica y de investigación española.

<https://www.rediris.es/cert/doc/unixsec/node7.html>

[Fecha de consulta: 12 de octubre de 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 142	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **ping**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**ping**

DEFINICIÓN

Ping: Utilidad de TCP/IP que se emplea para comprobar si se puede alcanzar otro host. Se envía una solicitud ICMP (Internet Control Message Protocol, Protocolo de mensajes de control de Internet) al host que responde si es alcanzable.

Ping de la muerte: Se envía un gran paquete ICMP (Internet Control Message Protocol, Protocolo de mensajes de control de Internet) para desbordar el búfer del host remoto. Suele hacer que este se reinicie o se quede colgado.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 143	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **polymorphic**	**REFERENCIA** *Seguridad informática CompTIA Segurity+. Guía de seguridad y certificación del examen SYO-301*
EQUIVALENTE	**polimórfico**
DEFINICIÓN Atributo de algunos virus que les permite mutar y aparecer de forma diferente cada vez que se presentan. Las mutaciones dificultan que los encuentren (y reaccionen) los escáneres.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 63	**AUTOR Y FECHA** **MJPM, 20 de agosto, 2016**
TÉRMINO **port scanner**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**escáner de puerto**
DEFINICIÓN Elemento (físico o de software) que escanea un servidor para encontrar puertos abiertos para aprovecharse de ellos. El escaneo de puertos es el proceso de enviar mensajes a puertos para ver cuáles están disponibles y cuáles no.	
FUENTE DE LA DEFINICIÓN	

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: NEOLOGISMOS.

FICHA Nº 64	**AUTOR Y FECHA** **MJPM, 20 de agosto, 2016**
TÉRMINO **PPP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**PPP**
DEFINICIÓN *Point-to-Point Protocol*, Protocolo punto a punto. Protocolo de nivel de enlace que sustituye a SLIP (Serial Line Internet Protocol, Protocolo de Internet de línea de serie). Es parte del entorno TCP/IP estándar y se suele utilizar en conexiones de marcado.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 65	**AUTOR Y FECHA** **MJPM, 20 de agosto, 2016**
TÉRMINO **PPTP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**PPTP**
DEFINICIÓN *Point-to-Point Tunneling Protocol*, Protocolo de túnel punto a punto. Extensión del protocolo PPP (*Point-to-Point Protocol*, Protocolo punto a punto) que se utiliza en redes VPN. Una opción alternativa es L2TP.	
FUENTE DE LA DEFINICIÓN	

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 145	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **protocol**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**protocolo**
DEFINICIÓN Estándar o regla.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 66	**AUTOR Y FECHA** **MJPM, 20 de agosto, 2016**
TÉRMINO **protocol analyzer**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**analizador de protocolo**
DEFINICIÓN Herramienta de resolución de problemas de hardware y software que se utiliza para decodificar la información del protocolo e intentar determinar el origen de un problema de red y establecer líneas de base. Analizador de protocolos de red: Dispositivo que accede a la señalización en el cable de red.	
FUENTE DE LA DEFINICIÓN	

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 146	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **proxy**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**proxy**
DEFINICIÓN Tipo de cortafuegos que evita las comunicaciones directas entre un cliente y un host actuando como intermediario. Véase también Cortafuegos. Cortafuegos: Combinación de hardware y software que protege una red frente a ataques realizados por piratas informáticos que podrían acceder a través de redes públicas, incluyendo Internet. Cortafuegos proxy: Servidor proxy que también actúa como cortafuegos, bloqueando el acceso de red desde redes externas.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 67	**AUTOR Y FECHA** **MJPM, 20 de agosto, 2016**
TÉRMINO **RADIUS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**RADIUS**
DEFINICIÓN *Remote Authentication Dial In User Service*, Servicio de autenticación remota telefónica de usuario. Mecanismo que permite la autenticación de conexiones remotas y otras redes. En principio, se ideó para conexiones de marcado, pero	

ha evolucionado mucho y tiene múltiples características modernas.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 144	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **remote access**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**acceso remoto**

DEFINICIÓN

Un acceso remoto es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet).

En el acceso remoto se ven implicados protocolos (En informática, un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes), y programas en ambas computadoras que permitan recibir/enviar los datos necesarios. Además deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y los programas).

Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras. Se pueden acceder a archivos, dispositivos periféricos (como impresoras), configuraciones, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

FUENTE DE LA DEFINICIÓN

Ayudas para docentes CISCO - Material didáctico.

<http://ayudasparadocentes.blogspot.com.es/2012/01/que-es-un-acceso-remoto.html>

[Fecha de consulta: 12 de octubre de 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

***** Tener en cuenta que se trata de una fuente de América Latina y solo sirve para entender el

término específico de Acceso Remoto, que ya ha sido comprobado en fuentes españolas.

FICHA Nº 113	AUTOR Y FECHA MJPM, 11 de septiembre, 2014
TÉRMINO **roaming**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**roaming**
DEFINICIÓN El concepto de roaming dispone de una utilización extendida en el ámbito de las comunicaciones móviles para designar a aquella capacidad, posibilidad que ostenta un teléfono celular de realizar y recibir llamados más allá de su área de cobertura, es decir, por ejemplo, si una persona sale de su país, viaja al exterior, gracias al roaming podrá seguir utilizando, la línea digamos, sin problemas y como si estuviese en su lugar de cobertura, a pesar que su compañía no tenga cobertura en ese país de destino.	
FUENTE DE LA DEFINICIÓN Mastermagazine - Revista especializada <http://www.mastermagazine.info/termino/4050.php> [Fecha de consulta: 20 de diciembre, 2016]	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 147	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **roaming profile**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**pefil roaming**
DEFINICIÓN Perfil que se descarga del servidor en cada inicio de sesión. Cuando un	

usuario se desconecta al final de una sesión, se realizan cambios y se recuerdan para la próxima vez que el usuario inicie sesión.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 68	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **role/rule-based access**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**rol/acceso basado en roles**
DEFINICIÓN El control de acceso basado en roles (RBAC) es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al superusuario. Mediante la aplicación de atributos de seguridad a procesos y usuarios, RBAC puede dividir las capacidades de superusuario entre varios administradores. La gestión de derechos de procesos se implementa a través de privilegios. La gestión de derechos de usuarios se implementa a través de RBAC.	
FUENTE DE LA DEFINICIÓN *Oracle. Guía de administración del sistema: servicios de seguridad.* <https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 148	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **router**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**enrutador**

DEFINICIÓN

Un dispositivo que conecta redes separadas, que reenvía un paquete de una red a otra basándose solo en la dirección de red del protocolo que se está utilizando. Un enrutador determina la mejor ruta para los paquetes de datos desde el origen a su destino.

Enrutador fronterizo: Enrutador utilizado para traducir de una estructura LAN a una WAN.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: NEOLOGISMOS.

FICHA Nº 133	**AUTOR Y FECHA** **MJPM, 15 de agosto, 2016**
TÉRMINO **topology**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**topología**

DEFINICIÓN

Una red informática está compuesta por equipos que están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y elementos de hardware (adaptadores de red y otros equipos que garantizan que los datos viajen correctamente). La configuración física, es decir la configuración espacial de la red, se denomina topología física.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 149	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **scanning**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**escaneo**
DEFINICIÓN Proceso que emplean los agresores para recopilar información sobre la configuración de una red. Escáner de puerto: Elemento (físico o de software) que escanea un servidor para encontrar puertos abiertos para aprovecharse de ellos. El escaneo de puertos es el proceso de enviar mensajes a puertos para ver cuáles están disponibles y cuáles no.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMOS.	

FICHA Nº 69	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **SCP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**SCP**
DEFINICIÓN *Secure Copy:* Copia segura. SCP significa copiado seguro del inglés secure copy, esto quiere decir que se copiara archivos de un ordenador a otro a través de una conexión segura y encriptada. El comando scp utiliza por defecto el puerto 22, y se conecta mediante un enlace encriptado ssh Se puede utilizar scp para copiar archivos de un ordenador local a otro remoto, también se puede copiar del remoto al local y también se puede copiar entre	

dos remotos, mientras estás conectado a un tercer ordenador, y el tráfico no pasará por el ordenador en que estás. Se puede usar scp en Linux, Mac y Windows.
FUENTE DE LA DEFINICIÓN Blog de experto en la materia. Guillermo Garrón. <https://www.garron.me/es/articulos/scp.html> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 70	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **scripting**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**scripting**
DEFINICIÓN (guión) Son una especie de pequeños programas que corren en las páginas de Internet y que sirven para realizar determinado tipo de tareas de manera automática, como por ejemplo el conectarse a Internet (login) o checar el correo electrónico.	
FUENTE DE LA DEFINICIÓN Glosario.net - Diccionario de términos técnicos <http://tecnologia.glosario.net/terminos-tecnicos-internet/script-1483.html> [Fecha de consulta: 12 de octubre de 2016]	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 71	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **security server**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**servidor de seguridad**
DEFINICIÓN Un servidor de seguridad es un mecanismo que sirve para controlar el flujo de tráfico IP entre dos redes. Los dispositivos de servidor de seguridad funcionan habitualmente en L3 (nivel 3) del modelo OSI, aunque algunos modelos también pueden funcionar a niveles superiores. Generalmente, un servidor de seguridad interno proporciona las ventajas siguientes: • Defensa de servidores internos contra ataques de red. • Aplicación de directivas de uso y acceso a la red. • Supervisión de tráfico y generación de alertas en caso de detección de patrones sospechosos. Es importante destacar que los servidores de seguridad mitigan solo algunos tipos de peligros. Generalmente, un servidor de seguridad no evita el daño que se puede infligir a un servidor con un problema de seguridad de software. Los servidores de seguridad se deben implementar como parte de una arquitectura de seguridad completa de la organización.	
FUENTE DE LA DEFINICIÓN Microsoft TechNet - Portal lingüístico (Base de datos terminológica) <https://www.microsoft.com/spain/technet/recursos/articulos/secmod155.mspx#EMF> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 72	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **security topology**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**topología de seguridad**

DEFINICIÓN

Una red informática está compuesta por equipos que están conectados entre sí mediante líneas de comunicación (cables de red, etc.) y elementos de hardware (adaptadores de red y otros equipos que garantizan que los datos viajen correctamente). La configuración física, es decir la configuración espacial de la red, se denomina topología física. Los diferentes tipos de topología son:

- Topología de bus
- Topología de estrella
- Topología en anillo
- Topología de árbol
- Topología de malla

La topología lógica, a diferencia de la topología física, es la manera en que los datos viajan por las líneas de comunicación. Las topologías lógicas más comunes son Ethernet, Red en anillo y FDDI.

FUENTE DE LA DEFINICIÓN

CCM - High-Tech

<http://es.ccm.net/contents/256-topologia-de-red>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 150	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **security zone**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**zona de seguridad**

DEFINICIÓN

Método para aislar un sistema de otros sistemas o redes.

FUENTE DE LA DEFINICIÓN

Glosario. Seguridad Informática. CompTIA Security+ (Títulos Especiales). 2011.

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 151	**AUTOR Y AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **server**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**servidor**

DEFINICIÓN

Servidor: Ordenador que proporciona recursos a los clientes de una red.

Servidor caché proxy: Implementación de un proxy Web. El servidor recibe una solicitud HTTP de un navegador Web en representación del terminal de envío. Cuando llega la respuesta, este servidor almacena en caché una copia de la respuesta de forma local. La próxima vez que alguien solicite la misma página Web o información de Internet, el servidor atenderá la solicitud desde la memoria caché en lugar de recuperar el recurso de la Web.

Servidor de tolerancia a fallos: Sistema de copia de seguridad para un sitio cálido en la que se conecta el servidor de tolerancia a fallos al servidor principal. El latido se envía de este al servidor de seguridad. Si el latido se detiene, se inicia el sistema de tolerancia a errores y asume el control. De este modo, el sistema no se interrumpe aunque el servidor principal no esté funcionando.

Servidor DNS: Cualquier servidor que lleve a cabo la resolución de direcciones desde un DNS FQDN (Fully Qualified Domain Name, Nombre de dominio plenamente cualificado) para una dirección IP. Véase también DNS e IP.

Servidor duplicado: Dos servidores idénticos que se utilizan para la agrupación en clústeres.

Servidor ilícito: Aplicación o programa que no debería pero está funcionando en la red. Se suele utilizar para obtener control no autorizado permitiendo que alguien sobrepase la autenticación normal. NetBus es uno de los ejemplos más conocidos de servidor ilícito.

Servidor no autorizado: Servidor DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración dinámica de host) activo que se ha añadido a la red y está cediendo direcciones a los usuarios en lugar de que éstos obtengan una dirección de su servidor.

Servidor proxy: Tipo de servidor que realiza una única conexión a Internet y solicitudes de servicios en representación de muchos usuarios.

Servidor Web: Servidor que guarda y entrega páginas Web y otro contenido Web utilizando HTTP. Véase también HTTP.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: NEOLOGISMO.

FICHA Nº 152	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **seven-layer OSI model**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**modelo de siete capas OSI**

DEFINICIÓN

Modelo OSI (Open System Interconnection, Modelo de interconexión de sistemas abiertos): Modelo definido por ISO para categorizar el proceso de la comunicación entre ordenadores en términos de siete capas. Ésas son Aplicación, Presentación, Sesión, Transporte, Red, Enlace de datos y Física. Véase también ISO.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 153	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **signal**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**señal**

DEFINICIÓN Transmisión de un ordenador a otro. Una señal podría ser una notificación para iniciar o finalizar una sesión.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 154	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **social engineering**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**ingeniería social**
DEFINICIÓN Ataque que utiliza a los demás para engañarlos. No se dirige de forma directa al hardware y al software, en su lugar, trata de manipular a las personas.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 155	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **spike**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**pico**
DEFINICIÓN Incremento momentáneo o instantáneo de la energía en una línea de	

corriente.

Conducto protector: Dispositivo que protege los componentes eléctricos de incrementos instantáneos o momentáneos (llamados picos) en una línea de corriente.

Regulador de energía: Dispositivo que condiciona el suministro eléctrico para desechar los picos repentinos.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 73	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **OSI model**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**modelo OSI**

DEFINICIÓN

Open System Interconnection, Modelo de interconexión de sistemas abiertos. Modelo definido por ISO para categorizar el proceso de la comunicación entre ordenadores en términos de siete capas. Ésas son Aplicación, Presentación, Sesión, Transporte, Red, Enlace de datos y Física. Véase también ISO.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 74	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **SFA**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**SFA**

DEFINICIÓN

Single factor authentication, Factor de autenticación único.

Proceso de validación de las credenciales de una persona, proceso informático o dispositivo. Para la autenticación se necesita que la persona, proceso o dispositivo que realiza la solicitud proporcione una credencial que demuestre que se trata en realidad de la entidad o persona que dice ser. Entre las formas habituales de credenciales se incluyen las firmas digitales, las tarjetas inteligentes, los datos biométricos y una combinación formada por los nombres de usuario y sus contraseñas.

FUENTE DE LA DEFINICIÓN

Microsoft TechNet - Portal lingüístico (Base de datos terminológica)

<https://technet.microsoft.com/es-es/library/cc875841.aspx>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 75	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **SFTP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**SFTP**

DEFINICIÓN

SFTP: *SSH, File Transfer Protocol,* Protocolo Seguro de transferencia de ficheros.

En informática, el SSH File Transfer Protocol, es un protocolo de red que provee acceso, administración y transferencia de archivos sobre un flujo de datos fiable (especialmente SSH).

En español, protocolo de transferencia de archivos SSH, también llamado Secure File Transfer Protocol o SFTP (aunque no debe ser confundido con el FTPS).

Fue diseñado por el IETF como extensión del protocolo SSH (Secure Shell) versión 2.0, para agregarle transferencia de archivos segura. Aunque es

independiente del SSH, por lo que también puede ser usado con otros protocolos, como ser transferencia de información de gestión en aplicaciones VPN, o transferencia de archivos seguros sobre TLS.
FUENTE DE LA DEFINICIÓN *ALGESA. Diccionario especializado.* <http://www.alegsa.com.ar/Dic/ssh%20file%20transfer%20protocol.php> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 76	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **single sign on**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**inicio de sesión único**
DEFINICIÓN Relación entre el cliente y la red en la que al cliente solo se le permite acceder una vez y todos los recursos se basan en ese inicio de sesión (al contrario que la necesidad de iniciar sesión en cada servidor individual para acceder a los recursos).	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMO.	

FICHA Nº 77	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **smart card**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**tarjeta inteligente**

DEFINICIÓN

Una tarjeta inteligente o tarjeta chip, consiste en un fragmento de plástico del tamaño de una tarjeta de crédito, con un microprocesador con memoria propia adosado. El componente principal que posee esa tarjeta inteligente es, sin lugar a dudas, el microchip interno.

FUENTE DE LA DEFINICIÓN

EcuRed - Diccionario especializado.

<https://www.ecured.cu/Tarjetas_Inteligentes>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 78	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **smart card reader**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**lector de tarjeta inteligente**

DEFINICIÓN

Las tarjetas son manipuladas por lectores fabricados para ese propósito en específico. Estos varían en potencialidades de acuerdo con el fabricante. Incluso pueden cambiar la forma de ser utilizados.

Existen lectores del tipo tontos, lo cual quiere decir que no poseen inteligencia propia, son simplemente instalados en una computadora y esta se encarga de su manipulación. De este tipo se pueden encontrar variantes internas (se colocan en una bahía de una torre de disco 3) y externas (conectadas por algún puerto a la máquina). Para el caso de las tarjetas sin contactos, existen variantes especiales de estos lectores.

Por otro lado están los Lectores autónomos, los cuales existen en múltiples variantes. Estos lectores poseen un Microchip interno que es el encargado de ejecutar las aplicaciones grabadas en la memoria que tiene. En su interior poseen, incluso, un sistema operativo propio (dependiente del fabricante), que es el encargado de soportar las distintas aplicaciones manejadoras de tarjetas inteligentes que se le instalen.

FUENTE DE LA DEFINICIÓN

EcuRed

<https://www.ecured.cu/Tarjetas_Inteligentes>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 79	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **SNA**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**SNA**

DEFINICIÓN

Systems Network Architecture: Arquitectura de sistemas de red. IBM creó SNA (System Network Architecture) en 1974, como una arquitectura de comunicaciones para redes predominantes basadas en mainframes. En lo referente a tecnología de mainframes nada cambia de la noche a la mañana, pero a mediados de los 80 SNA se había convertido en la solución dominante en las redes del entorno IBM. Es una arquitectura compleja pero que se comprende bien, y aunque su implantación resulta costosa es fiable, gestionable, predecible y segura.

La arquitectura SNA (System Network Architecture) de IBM define un conjunto de servicios y protocolos para la conectividad, interoperación y gestión de red. Los objetivos establecidos al definir SNA son básicamente los que se pretende con otras arquitecturas en niveles. En SNA, desde el primer momento se hizo énfasis en los siguientes aspectos que, con el tiempo, se están teniendo en consideración en otras arquitecturas: facilitar el desarrollo e instalación de sistemas y aplicaciones y la gestión y control total de la red.

FUENTE DE LA DEFINICIÓN

TECNOLOGÍA DE REDES - Blog de experto.

<http://latecnologiaderedes.blogspot.com.es/2011/05/asna_9841.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 80	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **sniffer**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**sniffer**
DEFINICIÓN Dispositivo físico que escucha el tráfico de red y busca elementos que puedan tener sentido. Hay un propósito legítimo para estos dispositivos: los administradores los utilizan para analizar el tráfico. Sin embargo, cuando los emplean otras personas que no son el administrador, se convierten en riesgos de seguridad.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 81	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **SNMP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**SNMP**
DEFINICIÓN *Simple Network Management Protocol*, Protocolo simple de administración de redes. Se trata de una herramienta de gestión que permite la comunicación entre dispositivos de red y una consola de administración.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 82	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **spam filter**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**filtro de spam**
DEFINICIÓN Las reglas o filtros de correo son utilidades del cliente de correo electrónico (Webmail, Outlook, Eudora, etc.) para organizar los mensajes recibidos. De esta forma, podemos utilizar estos filtros o reglas, además de para organizar nuestros mensajes en carpetas, para combatir el spam moviendo o eliminando aquellos mensajes que cumplan las condiciones especificadas en las reglas o filtros.	
FUENTE DE LA DEFINICIÓN Universidad de Granada - CSIRC <https://csirc.ugr.es/informatica/correoelectronico/MasInfo/ServicioAntispam/CrearReglasFiltros/> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: PRÉSTAMOS Y CALCOS.	

FICHA Nº 83	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **SSH**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**SSH**
DEFINICIÓN *Secure Shell*, Intérprete de órdenes seguro. Sustituto para rlogin en Unix/Linux que incluye seguridad. rlogin permitía a un host establecer una conexión con otro sin una seguridad real. SSH lo reemplaza con slogin y los certificados digitales.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 84	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **SSL**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**SSL**
DEFINICIÓN *Secure Sockets Layer*, Capa de zócalo seguro. Protocolo que asegura los mensajes operando entre las capas Aplicación (HTTP) y Transporte.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 85	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **standard**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**estándar**
DEFINICIÓN Una de las principales herramientas que han permitido a las distintas herramientas informáticas poder interactuar y así proporcionar una experiencia satisfactoria al usuario han sido los estándares. Los estándares, o parte de ellos como se comprobará en adelante, han sido la herramienta base de la interoperabilidad informática. Son los que han permitido definir cómo interactuaran los miles o millones de componentes informáticos que existen. Sin embargo, estándares existen de muchos tipos y según de cuál de ellos se	

esté hablando, se estarán garantizando unas funcionalidades y unas capacidades de interoperabilidad técnica distintas.

Así, los estándares se pueden clasificar en función de diversas características. Las dos principales probablemente, de cara a las implicaciones que tienen de cara a su uso son cómo de abiertos/cerrados y permisivos/exclusivos son, y qué carácter legal tienen. También es interesante observar qué organismo ha emitido y es responsable del estándar, así como su ámbito geográfico de aplicación. De hecho, se comprobará que las diferencias legales entre distintos entornos geopolíticos, van a determinar que un determinado estándar pueda ser considerado diferentemente dependiendo del lugar donde se emplee o comercialice.

Sin embargo, y fuera de toda categoría, un estándar, para poder denominarse como tal, al menos requiere cumplir una característica: sus especificaciones son públicas y accesibles cuando más a un precio simbólico. La especificación de un estándar, a su vez, es aquel conjunto de documentos donde se define cómo llevar a cabo un desarrollo de software o hardware que siga ese estándar.

FUENTE DE LA DEFINICIÓN

"Estudio sobre Estándares Informáticos tipos y caracterizaciones".
<http://datateca.unad.edu.co/contenidos/15001/Lecturas/Estandar_informatico_y_sus_tipos.pdf>
[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: NEOLOGISMO.

FICHA Nº 86	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **subnetting**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**subnetting**

DEFINICIÓN

La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

El Subneteo permite una mejor administración, control del tráfico y seguridad

al segmentar la red por función. También, mejora la performance de la red al reducir el tráfico de broadcast de nuestra red. Como desventaja, su implementación desperdicia muchas direcciones, sobre todo en los enlaces seriales.

FUENTE DE LA DEFINICIÓN

ADMINISTRACIÓN Y GESTIÓN DE REDES - Blog especializado.

<http://administracion-y-gestion-de redes.blogspot.com.es/p/subnetting_06.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 87	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **switch**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**switch**

DEFINICIÓN

Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de datos del modelo OSI. 2.) Término general que se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

FUENTE DE LA DEFINICIÓN

Glosario.net - Diccionario de términos técnicos.

<http://tecnologia.glosario.net/terminos-tecnicos-internet/switch-1557.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 88	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **TACACS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**TACACS**
DEFINICIÓN *Terminal Access Controller Access Control System*, Sistema de control de acceso mediante control del acceso desde terminales. Sistema de autenticación que permite que acepten credenciales procedentes de varios métodos, incluyendo Kerberos. El proceso cliente/servidor TACACS se produce del mismo modo que el proceso RADIUS (Remote Authentication Dial In User Service, Servicio de autenticación remota telefónica de usuario).	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 89	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **TACACS+**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**TACACS+**
DEFINICIÓN *Terminal Access Controller Access Control System:* Servicio de autenticación remota telefónica de usuario. El TACACS+ es un protocolo cliente/servidor que proporciona la Seguridad centralizada para los usuarios que intentan tener el Acceso de administración a un router o a un servidor de acceso a la red. El TACACS+ proporciona estos servicios del Authentication, Authorization, and Accounting (AAA): - Autenticación de los usuarios que intentan iniciar sesión al equipo de red - Autorización de determinar qué nivel de usuarios del acceso debe tener	

- El considerar para no perder de vista todos los cambios el usuario hace
FUENTE DE LA DEFINICIÓN CISCO Networking Academy. <http://www.cisco.com/cisco/web/support/LA/112/1125/1125952_117711-config-tacacs-00.html> [Fecha de consulta: 12 de octubre, 2016]
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 90	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **TCP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE **TCP**	
DEFINICIÓN Transmission Control Protocol, Protocolo de control de transmisión): El protocolo que se encuentra en la capa Host a host del modelo del Departamento de Defensa. Este protocolo descompone los paquetes de datos en segmentos, los numera y los envía en orden. El ordenador receptor vuelve a ensamblar los datos para que el usuario pueda leer la información. En este proceso, el emisor y el receptor confirman que han recibido todos los datos. De lo contrario, se vuelven a enviar. TCP es un protocolo orientado a la conexión. Véase también Orientado a conexión.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 91	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **TCP/IP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam*

	SY0-301, 5th Edition. 2011.
EQUIVALENTE	**TCP/IP**
DEFINICIÓN *Transmission Control Protocol/Internet Protocol*, Protocolo de control de acceso/Protocolo de Internet. Entorno de protocolo desarrollado por el Departamento de Defensa en combinación con Internet. Se diseñó como entorno de protocolo de interconexión de red para dirigir información sobre fallos de red. Hoy en día es el estándar que utiliza para las comunicaciones en Internet.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 92	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **TELNET**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**TELNET**
DEFINICIÓN Protocolo que funciona en la capa Aplicación del modelo OSI, proporcionando capacidades de simulación del terminal. Véase también Modelo OSI.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 93	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **thelephony**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**telefonía**

DEFINICIÓN

La telefonía IP le proporciona una manera de dotar de servicios consistentes a todos sus empleados en sus lugares de trabajo, tanto si están en la oficina o conectados remotamente. La telefonía IP transmite comunicaciones de voz a través de la red mediante la utilización de los estándares del protocolo de internet

La telefonía IP de Cisco son parte integral de la solución de Comunicaciones Unificadas de Cisco, que unifican voz, vídeo, datos, y aplicaciones móviles en redes tanto fijas como móviles, capacitando a los usuarios para comunicarse fácilmente en su lugar de trabajo a través de cualquier medio, dispositivo o sistema operativo.

Utilizando la red como plataforma, la telefonía IP de Cisco ayuda a organizaciones de todos los tamaños a conseguir mayor seguridad, resistencia, flexibilidad y escalabilidad, además de los beneficios inherentes de usar una red convergente para el transporte de datos y la interconexión.

FUENTE DE LA DEFINICIÓN

CISCO - CISCO Networking Academy.

<http://www.cisco.com/c/es_es/products/unified-communications/telefonia-ip.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 156	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **TKIP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.

EQUIVALENTE	**TKIP**

DEFINICIÓN

TKIP (Temporal Key Interchange/Integrity Protocol, Protocolo de intercambio/integridad de claves temporal): Contenedor que funciona con el cifrado inalámbrico para fortalecer las conexiones WEP. Se diseñó para proporcionar un cifrado más seguro que WEP.

FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 94	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **TLS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**TLS**
DEFINICIÓN *Transport Layer Security*, Seguridad de la capa Transporte. Protocolo cuyo propósito es verificar que las conexiones seguras entre un servidor y un cliente siguen siendo seguras. Se define en RFC 2246.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 157	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **token**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**token**
DEFINICIÓN Token: Pieza de datos que contiene información sobre el usuario. Puede contener ID de grupo, de usuario o nivel de privilegios, entre otros. Token de seguridad: Pieza de datos que contiene los derechos y privilegios de acceso del portador del token.	

FUENTE DE LA DEFINICIÓN Glosario. Seguridad Informática. CompTIA Security+ (Títulos Especiales). 2011.
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 95	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **trusted OS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**SO de confianza**
DEFINICIÓN Un Sistema Operativo (SO) es el software básico de una computadora que provee una interfaz entre el resto de programas del computador, los dispositivos hardware y el usuario. Las funciones básicas del Sistema Operativo son administrar los recursos de la máquina, coordinar el hardware y organizar archivos y directorios en dispositivos de almacenamiento. Los Sistemas Operativos más utilizados son Dos, Windows, Linux y Mac. Algunos SO ya vienen con un navegador integrado, como Windows que trae el navegador Internet Explorer.	
FUENTE DE LA DEFINICIÓN TECNOLOGÍA E INFORMÁTICA – Blog. <https://solvasquez.wordpress.com/2011/01/24/definicion-de-sistema-operativo/> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 96	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **tunneling**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**tunelado**
DEFINICIÓN Acto de enviar datos a través de una red pública encapsulándola en otros paquetes.	
FUENTE DE LA DEFINICIÓN Glosario. Seguridad Informática. CompTIA Security+ (Títulos Especiales). 2011.	
OBSERVACIONES: NEOLOGISMO.	

FICHA Nº 97	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **UDP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**UDP**
DEFINICIÓN *User Datagram Protocol*, Protocolo de datagramas de usuario. En la capa Host a host, el protocolo TCP/IP del Departamento de Defensa, que corresponde a la capa Transporte del modelo OSI. Los paquetes se dividen en datagramas, dados los números se envían y se vuelven a unir en el lado del receptor. UDP es un protocolo sin protección. Véase también Modelo OSI.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 158	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **UPS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**UPS**
DEFINICIÓN UPS (Uninterruptible Power Supply, Sistema de alimentación ininterrumpida): Dispositivo que proporciona energía a corto plazo, normalmente utilizando baterías.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 159	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **user**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**usuario**
DEFINICIÓN Persona que está utilizando un ordenador, red o recurso.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 98	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **virtualization**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**virtualización**
DEFINICIÓN Virtualizar es multiplexar o abstraer un recurso. La virtualización es el proceso de presentar un subconjunto de recursos físicos agrupados de forma lógica, de tal forma que se obtengan beneficios sobre la configuración original. Combinación de hardware y software que permite a un recurso físico funcionar como múltiples recursos lógicos. • Podemos definirla también como “la abstracción o la multiplexación de un recurso físico”. ◦ Todas las tecnologías de virtualización tienen como factor común el ocultar detalles técnicos a través de la encapsulación. ◦ La virtualización crea un interfaz externo que esconde una implementación subyacente.	
FUENTE DE LA DEFINICIÓN IES Gonzalo Nazareno. <http://www.gonzalonazareno.org/cloud/material/IntroVirtualizacion.pdf> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: NEOLOGISMO.	

FICHA Nº 99	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **VLAN**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**VLAN**
DEFINICIÓN	

Virtual LAN, LAN virtual. Red de área local que permite a los usuarios de distintos puertos de comunicación participar en su propia red independiente pero siguen estando conectados a las otras estaciones en el mismo conmutador o uno conectado.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 100	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **VPN**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**VPN**
DEFINICIÓN *Virtual Private Network*, Red privada virtual. Sistema que utiliza Internet como base para una interconexión privada (red) entre dos localizaciones.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 101	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **web security gateways**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**puerta de enlace de seguridad web**
DEFINICIÓN La comunicación Web en IBM® Cognos Controller se establece normalmente a	

través de puertas de enlace, que residen en uno o más servidores Web. Una puerta de enlace es una extensión de un programa de servidor Web que transfiere información del servidor Web a otro servidor.

La comunicación Web puede establecerse directamente con Controller Web Services Server Controller Web Services Server o el distribuidor de Report Server Distribuidor. Esto puede mejorar el rendimiento en los entornos en los que la puerta de enlace no es obligatoria por motivos de seguridad.

Si instala el componente de puerta de enlace en una máquina distinta a la de los componentes de servidor de IBM Cognos Controller, debe configurar la máquina de puerta de enlace de modo que pueda conocer la ubicación de un Controller Client Distribution Server.

FUENTE DE LA DEFINICIÓN

IBM Knowledge Center.

<http://www.ibm.com/support/knowledgecenter/es/SSWGNW_10.1.0/com.ibm.swg.ba.cognos.ctrl_arch.10.1.1.doc/c_cntl_gateway.html>

[Fecha de consulta: 12 de octubre, 2016]

OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.

FICHA Nº 160	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **WEP**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. 2011.
EQUIVALENTE	**WEP**

DEFINICIÓN

WEP (Wired Equivalent Privacy, Privacidad equivalente a cableado): Protocolo de seguridad para redes 802.11b (inalámbrico) que intentan establecer la misma seguridad que si se tratara de conexiones de cableado.

FUENTE DE LA DEFINICIÓN

Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.

OBSERVACIONES: SIGLAS Y ACRÓNIMOS.

FICHA Nº 161	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **Wi-Fi**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**Wi-Fi**
DEFINICIÓN Wi-Fi (Wireless Fidelity, Fidelidad inalámbrica): Red inalámbrica que funciona en el rango de 2.4 a 5 Ghz.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 164	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **wireless access point**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**punto de acceso inalámbrico**
DEFINICIÓN Puente inalámbrico utilizando una red de frecuencia de radio multipunto.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

FICHA Nº 162	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **WPA**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**WPA**
DEFINICIÓN WPA (Wi-Fi Protected Access, Acceso protegido Wi-Fi): Protocolo de seguridad desarrollado por la Alianza Wi-Fi para proteger a las redes inalámbricas y superar lo que ofrecía WEP. Hay dos versiones, WPA y WPA 2, esta última es la implementación completa de las características de seguridad.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 163	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **WTLS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**WTLS**
DEFINICIÓN WTLS (Wireless Transport Layer Security, Seguridad para la capa de transporte en comunicaciones inalámbricas): Capa de seguridad de WAP (Wireless Applications Protocol, Protocolo de aplicaciones inalámbricas). WTLS proporciona autenticación, cifrado e integridad de datos para dispositivos inalámbricos.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 102	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **XTACACS**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**XTACACS**
DEFINICIÓN El TACACS+ (XTACACS) es un protocolo cliente/servidor que proporciona la Seguridad centralizada para los usuarios que intentan tener el Acceso de administración a un router o a un servidor de acceso a la red. El TACACS+ proporciona estos servicios del Authentication, Authorization, and Accounting (AAA): Autenticación de los usuarios que intentan iniciar sesión al equipo de red Autorización de determinar qué nivel de usuarios del acceso debe tener El considerar para no perder de vista todos los cambios el usuario hace	
FUENTE DE LA DEFINICIÓN CISCO - CISCO Networking Academy. <http://www.cisco.com/cisco/web/support/LA/112/1125/1125952_117711-config-tacacs-00.html> [Fecha de consulta: 12 de octubre, 2016]	
OBSERVACIONES: SIGLAS Y ACRÓNIMOS.	

FICHA Nº 165	AUTOR Y FECHA MJPM, 12 de octubre, 2016
TÉRMINO **zombie**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**zombie**
DEFINICIÓN Cualquier sistema que utilice las direcciones de un ordenador de control maestro. Los zombies se suelen utilizar en ataques DDoS (Distributed Denial-	

of-Service, Denegación de servicio distribuida) y botnet.
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.
OBSERVACIONES: PRÉSTAMOS Y CALCOS.

FICHA Nº 103	**AUTOR Y FECHA** **MJPM, 12 de octubre, 2016**
TÉRMINO **zone**	**REFERENCIA** *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301,* 5th Edition. 2011.
EQUIVALENTE	**zona**
DEFINICIÓN Área de un edificio en la que se puede monitorizar y controlar de forma individual.	
FUENTE DE LA DEFINICIÓN Glosario. *Seguridad Informática. CompTIA Security+* (Títulos Especiales). 2011.	
OBSERVACIONES: TRADUCCIÓN POR EQUIVALENCIA.	

6.3. Glosario bilingüe

A continuación presentamos el glosario bilingüe realizado a partir de las fichas terminológicas confeccionadas. Cabe destacar que el glosario que hemos desarrollado es mucho más amplio y que este es solo una muestra de los términos más significativos de los dos capítulos objeto de análisis en este trabajo de investigación.

GLOSARIO INGLÉS-ESPAÑOL DE TÉRMINOS RELACIONADOS CON LA SEGURIDAD INFORMÁTICA		
Nº de ficha	**Término en inglés**	**Término en español**
1	access control	control de acceso
2	ACL	ACL
105	add-on	complemento
106	adware	adware
107	algorithm	algoritmo
3	attachment	adjunto
108	attack	ataque
109	authentication	autenticación
4	authorization	autorización
110	bastion host	host de bastión
111	biometrics	biometría
112	biometrics devices	dispositivos biométricos
113	bit	bit
114	bot	bot
7	BPN	BPN
8	broadcast	transmisión
9	buffer	búfer
10	buffer overflow	desbordamientos de búfer

115	CCTV	CCTV
116	CHAP	CHAP
11	CIA (Confidentiality, integrity and availability)	CIA (Confidencialidad, integridad y disponibilidad)
117	client	cliente
12	common access card	tarjeta de acceso común
13	cookie	cookie
14	cross-site scripting	filtro de scripts de sitios
15	DAC (Discretionary access control)	DAC (Control de acceso discrecional)
16	datagram	datagrama
17	digital	digital
118	DMZ	DMZ
18	DNS	DNS
119	DSSS	DSSS
120	EMI	EMI
121	encryption	cifrado
19	ethernet	ethernet
122	extranet	extranet
20	extrusion	extrusión
123	FHSS	FHSS
124	firewall	cortafuegos
21	FTP	FTP
22	FTPS	FTPS
23	gateway	puerta de enlace
125	hacker	hacker
24	honeynet	honeynet
126	honeypot	honeypot

127	host	host
25	HTTP	HTTP
26	HTTPS	HTTPS
27	hub	concentrador
128	HVAC	HVAC
28	IANA	IANA
29	ICMP	ICMP
30	identification	identificación
129	IDS	IDS
130	IEEE 802.11x	IEEE 802.11x
31	implicit deny	denegación implícita
131	Internet	Internet
32	Intranet	Intranet
33	IP	IP
34	IPS	IPS
132	IPSec	IPSec
35	IPv4	IPv4
36	IPv6	IPv6
37	IPX	IPX
38	ISDN	ISDN
133	ISP	ISP
134	Kerberos	Kerberos
40	L2TP	L2TP
41	LAN	LAN
42	LDAP	LDAP
43	link	enlace
44	load balancers	balanceo de carga

45	login	login
46	logon	logon
135	MAC	MAC
136	MAC address	dirección MAC
47	malicious add-ons	complementos maliciosos
48	mandatory access control	control de acceso obligatorio
137	mantrap	mantrap
49	modem	módem
50	multicasting	multidifusión
51	Multihoming	Multihoming
52	NAC	NAC
53	NAT	NAT
54	NCP	NCP
55	NetBIOS	NetBIOS
138	network	red
56	network segmentation	
57	NIC	NIC
58	NIDS	NIDS
59	NIPS	NIPS
139	partitioning	particionamiento
60	password	contraseña
61	PBX system	sistema PBX
140	perimeter	perímetro
62	personal identification verification card	tarjeta de verificación de identificación personal
141	physical barriers	barreras físicas
142	ping	ping

143	polymorphic	polimórfico
63	port scanner	escáner de puerto
64	PPP	PPP
65	PPTP	PPTP
145	protocol	protocolo
66	protocol analyzer	analizadores de protocolo
146	proxy	proxy
67	RADIUS	RADIUS
144	remote access	acceso remoto
113	roaming	roaming
147	poaming profile	perfil roaming
68	role/rule-based access	rol/acceso basado en roles
148	router	enrutador
149	scanning	escaneo
69	SCP	SCP
70	scripting	scripting
71	security server	servidor de seguridad
72	security topology	topología de seguridad
150	security zone	zona de seguridad
151	server	servidor
152	seven-layer OSI model	modelo de siete capas OSI
74	SFA (Single factor authentication)	SFA (Factor de autenticación único)
75	SFTP	SFTP
153	signal	Señal
76	single sign on	inicio de sesión único
77	smart card	tarjeta inteligente

78	smart card reader	lector de tarjeta inteligente
79	SNA	SNA
80	sniffer	sniffer
81	SNMP	SNMP
154	social engineering	ingeniería social
82	spam filter	filtro de spam
155	spike	pico
83	SSH (Secure Shell)	SSH
84	SSL	SSL
85	standard	estándar
86	subnetting	subnetting
87	switch	switch
88	TACACS	TACACS
89	TACACS+	TACACS+
90	TCP	TCP
91	TCP/IP	TCP/IP
92	TELNET	TELNET
93	thelephony	telefonía
156	TKIP	TKIP
94	TLS	TLS
157	token	token
133	topology	topología
95	trusted OS	SO de confianza
96	tunneling	tunelado
158	UPS	UPS
159	user	usuario
97	UDP	UDP

160	WEP	WEP
161	Wi-Fi	Wi-Fi
162	WPA	WPA
163	WTLS	WTLS
164	wireless access point	punto de acceso inalámbrico
98	virtualization	virtualización
99	VLAN	VLAN
165	VPN concentrators	Concentradores VPN
101	web security gateways	puerta de enlace de seguridad web
102	XTACACS	XTACACS
166	zombie	zombie
103	zone	zona

6.4 Sistema de conceptos

Como afirma Belda Medina (2003: 328)[40], el crecimiento desbordante en el ámbito científico-técnico ha ido aparejado con la aparición en España de trabajos de investigación lingüística que estudian la relación entre ciencia, lenguaje y técnicas desde vertientes distintas: didáctica, discursiva, textual, pragmática, cognitiva, traductológica, terminológica, terminográfica, etc.[41] Muchos de estos trabajos han sido realizados por profesores de lenguas de especialidad, dado que son testigos de la intensa interrelación existente entre lenguaje y ciencia. Además, hay un buen número de filólogos, sensibles a los nuevos cambios que la sociedad reclama, que han abierto una vía muy interesante en el ámbito de la filología tradicional y han tratado de incorporar

[40] J. R. BELDA MEDINA: *El lenguaje de la informática e Internet y su traducción*. Alicante: Universidad de Alicante, 2003.

[41] Una útil e interesante síntesis de muchas de estas diferentes perspectivas, aplicadas al inglés profesional y académico, se encuentra en Alcaraz (2000). Para una relación muy completa de los trabajos realizados desde el año 1985, véase el reciente libro publicado por la profesora Bueno (2003), en donde se muestran, además, diferentes estadísticas por áreas, universidades, publicaciones, etc.

estas nuevas líneas de investigación, antes relegadas en el mundo de la filología tradicional en España.

Una de las herramientas surgida de estos estudios son los "mapas conceptuales", resultado de un proyecto de investigación con estudiantes de educación básica, llevado a cabo por el doctor Joseph D. Novak en el año 1972. Al parecer, se obtuvieron resultados muy fructíferos y, a partir de su publicación en la revista *AREA Journal*, han sido utilizados con diversos fines dentro de la enseñanza.

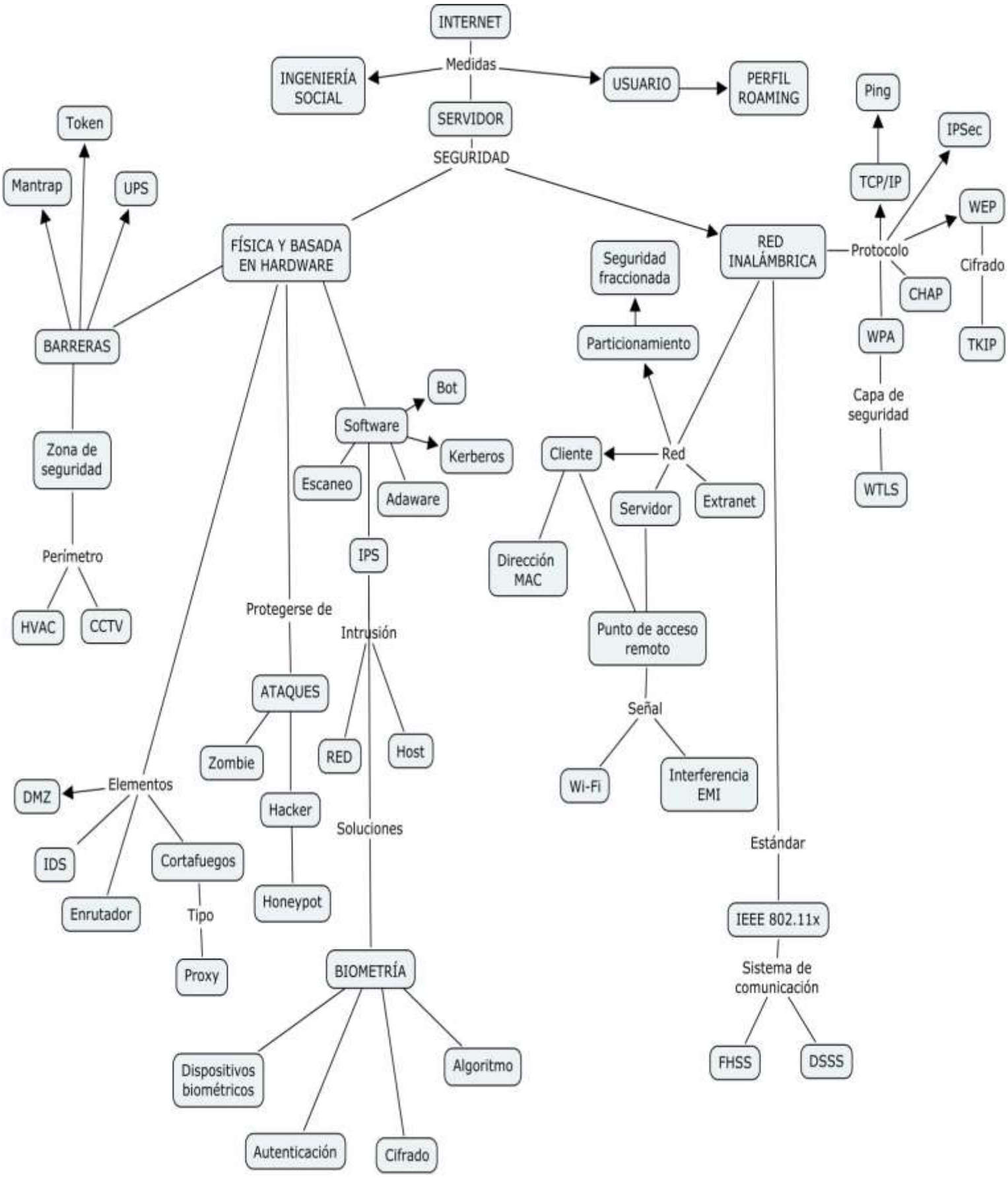
Entre otras utilidades, los mapas conceptuales se usan para analizar documentos escritos y extraer los significados de un campo de trabajo. Son considerados un medio para visualizar conceptos y las relaciones jerárquicas que existen entre ellos.

La construcción de un mapa conceptual implica:

1. Una atenta lectura del texto.
2. La identificación de las principales ideas o palabras clave con las que se construirá el mapa y su jerarquización.
3. La determinación de sus relaciones.
4. El uso adecuado de la simbología.
    - Las ideas o conceptos aparecen encerrados en un óvalo.
    - Los conectores indican la relación entre dos ideas y se representan a través de una línea que puede ser inclinada, horizontal o vertical.
    - Los descriptores son la palabra o palabras (máximo de tres) que se escriben cerca de los conectores o sobre ellos. Su función es "etiquetar" la relación.

El primer paso para comprender un texto es leerlo varias veces y centrar la atención en sus principales ideas y conceptos para darle significado.

Con el fin de realizar una lectura consciente del texto, hemos desarrollado el siguiente mapa conceptual de los principales conceptos que en él se describen. Cada uno de los términos que aparecen en este mapa conceptual ha sido previamente presentado en el fichero terminológico.


INTERNET
Medidas
INGENIERÍA SOCIAL
USUARIO
PERFIL ROAMING
SERVIDOR
SEGURIDAD
Token
Mantrap
UPS
FÍSICA Y BASADA EN HARDWARE
RED INALÁMBRICA
Ping
IPSec
TCP/IP
WEP
Protocolo
Cifrado
CHAP
Seguridad fraccionada
Particionamiento
WPA
TKIP
BARRERAS
Capa de seguridad
WTLS
Bot
Software
Kerberos
Escaneo
Adaware
Cliente
Red
Servidor
Extranet
Zona de seguridad
Perímetro
HVAC
CCTV
IPS
Dirección MAC
Protegerse de
Intrusión
Punto de acceso remoto
Señal
ATAQUES
Zombie
RED
Host
Wi-Fi
Interferencia EMI
DMZ
Elementos
Hacker
Soluciones
Estándar
IDS
Cortafuegos
Enrutador
Tipo
Honeypot
IEEE 802.11x
Proxy
BIOMETRÍA
Sistema de comunicación
Dispositivos biométricos
Algoritmo
FHSS
DSSS
Autenticación
Cifrado

7. APLICACIÓN DEL PROYECTO TERMINOLÓGICO EN EL PROCESO DE TRADUCCIÓN

7.1. Fases de creación de bases de datos en Multiterm a partir de un glosario en Excel

Una base de datos terminológica[42] se puede definir como una colección de datos sobre términos y conceptos de forma estructurada y legible electrónicamente. Dicho de otro modo, una base de datos terminológica es una base de datos lingüística en la que se almacenan términos propios del lenguaje técnico de un área particular de especialización. En nuestro caso, almacenamos términos del área de la seguridad informática y sus equivalentes en español, así como su definición.

En muchas ocasiones, los traductores pueden recibir glosarios en un archivo Excel o en un archivo de texto delimitado por tabulaciones (.txt) como parte del material de referencia de un proyecto. En este caso, como hemos mencionado en numerosas ocasiones a lo largo del presente trabajo de investigación, es el propio traductor especializado el encargado de elaborar la base de datos terminológica. Cuando se trata de listas de términos muy extensas es realmente laborioso buscar continuamente la terminología durante el proceso de traducción. Además, como cabe imaginar, es algo que consume bastante tiempo y puede llevar a alguna incoherencia terminológica. Por ello, si en nuestra labor de traducción trabajamos con la herramienta de traducción asistida por ordenador Trados 2014[43] o con cualquiera de las versiones de SDL Trados Studio, lo más eficaz es crear una base de datos con la herramienta de gestión terminológica Multiterm[44].

Para nuestra base de datos terminológica nos hemos decantado por la versión de Trados y Multiterm 2014, ya que es la versión más actualizada que tenemos a disposición. Cabe destacar que este proceso se puede realizar de

[42] Véase: Asociación Española de Terminología.
URL: <http://www.aeter.org/?page_id=75> [Fecha de consulta: 21 de diciembre, 2016]

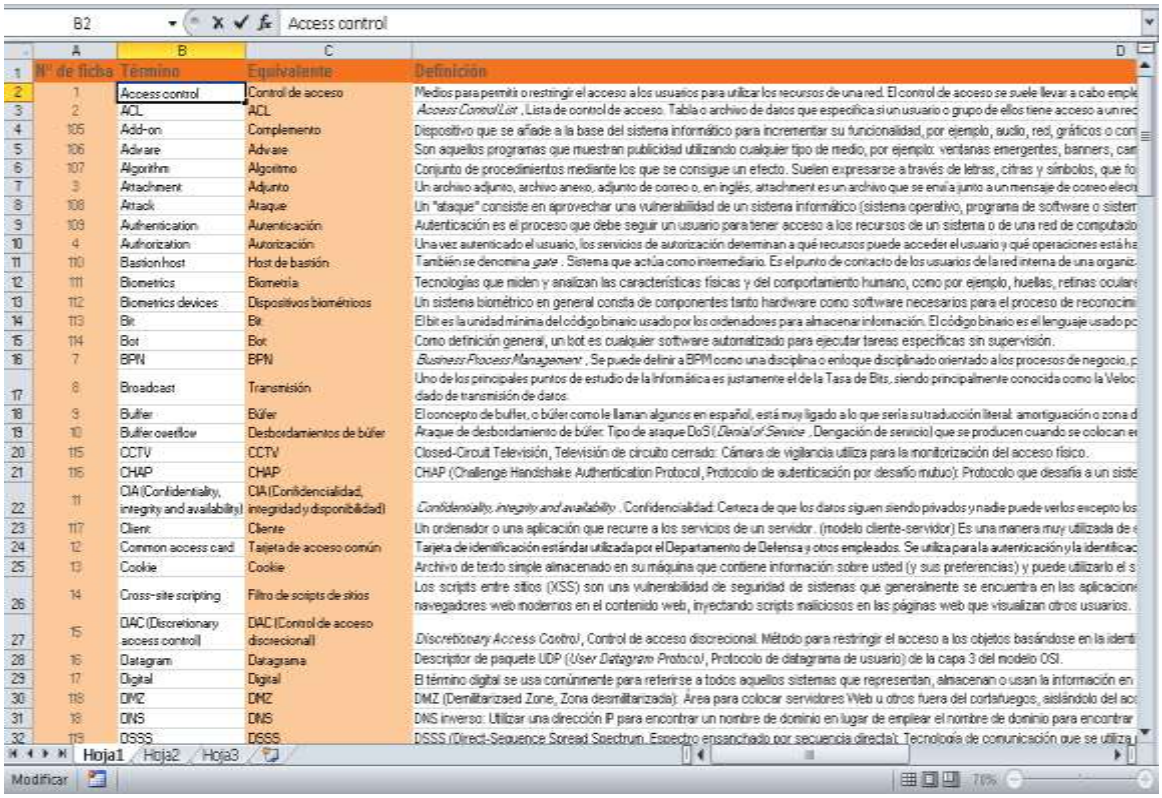
[43] SDL Trados Studio es un completo entorno de traducción para lingüistas profesionales que desean editar, revisar y gestionar proyectos de traducción, así como terminología corporativa.

[44] SDL MultiTerm Desktop es una herramienta de gestión terminológica de escritorio que funciona desde una base de datos central.

igual forma con versiones anteriores de ambos programas y que la última versión de Trados y Multiterm es la que se publicará en 2017.[45]

Crear una base de datos terminológica en Multiterm conlleva un proceso elaborado y delicado que merece la pena realizar por las numerosas ventajas que ofrece al traductor especializado y el incremento exponencial de la calidad de las traducciones ofrecidas. Repasemos, pues, las fases de la creación de la base de datos terminológica.

En primer lugar, como se ha observado en un capítulo anterior, se procede a la elaboración de las fichas terminológicas. El modelo de ficha elegido es sencillo con el fin de ajustarse de forma eficaz a las necesidades del encargo. Una vez que hemos elaborado las fichas, es preciso elaborar un glosario terminológico (en este caso, de inglés a español) en un archivo de Microsoft Excel (nosotros hemos utilizado la versión 2010, como ilustra la siguiente figura; no obstante, se pueden utilizar otras versiones).



	A	B	C	D
1	Nº de ficha	Término	Equivalente	Definición
2	1	Access control	Control de acceso	Medios para permitir o restringir el acceso a los usuarios para utilizar los recursos de una red. El control de acceso se suele llevar a cabo emple
3	2	ACL	ACL	*Access Control List* . Lista de control de acceso. Tabla o archivo de datos que especifica si un usuario o grupo de ellos tiene acceso a un rec
4	105	Add-on	Complemento	Dispositivo que se añade a la base del sistema informático para incrementar su funcionalidad, por ejemplo, audio, red, gráficos o con
5	106	Adware	Adware	Son aquellos programas que muestran publicidad utilizando cualquier tipo de medio, por ejemplo: ventanas emergentes, banners, cam
6	107	Algorithm	Algoritmo	Conjunto de procedimientos mediante los que se consigue un efecto. Suelen expresarse a través de letras, cifras y símbolos, que fo
7	3	Attachment	Adjunto	Un archivo adjunto, archivo anexo, adjunto de correo o, en inglés, attachment es un archivo que se envía junto a un mensaje de correo electr
8	108	Attack	Ataque	Un "ataque" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistem
9	109	Authentication	Autenticación	Autenticación es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computado
10	4	Authorization	Autorización	Una vez autenticado el usuario, los servicios de autorización determinan a qué recursos puede acceder el usuario y qué operaciones está ha
11	110	Bastion host	Host de bastión	También se denomina *gate* . Sistema que actúa como intermediario. Es el punto de contacto de los usuarios de la red interna de una organiz
12	111	Biometrics	Biometría	Tecnologías que miden y analizan las características físicas y del comportamiento humano, como por ejemplo, huellas, retinas ocular
13	112	Biometrics devices	Dispositivos biométricos	Un sistema biométrico en general consta de componentes tanto hardware como software necesarios para el proceso de reconocimi
14	113	Bit	Bit	El bit es la unidad mínima del código binario usado por los ordenadores para almacenar información. El código binario es el lenguaje usado pc
15	114	Bot	Bot	Como definición general, un bot es cualquier software automatizado para ejecutar tareas específicas sin supervisión.
16	7	BPN	BPN	*Business Process Management* . Se puede definir a BPM como una disciplina o enfoque disciplinado orientado a los procesos de negocio, p
17	8	Broadcast	Transmisión	Uno de los principales puntos de estudio de la Informática es justamente el de la Tasa de Bits, siendo principalmente conocida como la Veloc dado de transmisión de datos.
18	9	Buffer	Búfer	El concepto de buffer, o búfer como le llaman algunos en español, está muy ligado a lo que sería su traducción literal: amortiguación o zona d
19	10	Buffer overflow	Desbordamientos de búfer	Ataque de desbordamiento de búfer. Tipo de ataque DoS (*Denial of Service* . Dengación de servicio) que se producen cuando se colocan e
20	115	CCTV	CCTV	Closed-Circuit Televisión, Televisión de circuito cerrado: Cámara de vigilancia utiliza para la monitorización del acceso físico.
21	116	CHAP	CHAP	CHAP (Challenge Handshake Authentication Protocol, Protocolo de autenticación por desafío mutuo): Protocolo que desafía a un siste
22	11	CIA (Confidentiality, integrity and availability)	CIA (Confidencialidad, integridad y disponibilidad)	*Confidentiality, integrity and availability* . Confidencialidad: Certeza de que los datos siguen siendo privados y nadie puede verlos excepto los
23	117	Client	Cliente	Un ordenador o una aplicación que recurre a los servicios de un servidor. (modelo cliente-servidor) Es una manera muy utilizada de
24	12	Common access card	Tarjeta de acceso común	Tarjeta de identificación estándar utilizada por el Departamento de Defensa y otros empleados. Se utiliza para la autenticación y la identificac
25	13	Cookie	Cookie	Archivo de texto simple almacenado en su máquina que contiene información sobre usted (y sus preferencias) y puede utilizarlo el s
26	14	Cross-site scripting	Filtro de scripts de sitios	Los scripts entre sitios (XSS) son una vulnerabilidad de seguridad de sistemas que generalmente se encuentra en las aplicacion navegadores web modernos en el contenido web, inyectando scripts maliciosos en las páginas web que visualizan otros usuarios.
27	15	DAC (Discretionary access control)	DAC (Control de acceso discrecional)	*Discretionary Access Control*, Control de acceso discrecional. Método para restringir el acceso a los objetos basándose en la identi
28	16	Datagram	Datagrama	Descriptor de paquete UDP (*User Datagram Protocol*, Protocolo de datagrama de usuario) de la capa 3 del modelo OSI.
29	17	Digital	Digital	El término digital se usa comúnmente para referirse a todos aquellos sistemas que representan, almacenan o usan la información en
30	118	DMZ	DMZ	DMZ (Demilitarized Zone, Zona desmilitarizada): Área para colocar servidores Web u otros fuera del cortafuegos, aislándolo del ac
31	18	DNS	DNS	DNS inverso: Utilizar una dirección IP para encontrar un nombre de dominio en lugar de emplear el nombre de dominio para encontrar
32	119	DSSS	DSSS	DSSS (Direct-Sequence Spread Spectrum, Espectro ensanchado por secuencia directa): Tecnología de comunicación que se utiliza

Figura 15. Glosario terminológico EN-ES en un archivo de Excel 2010.

[45] Para acceder a información actualizada sobre la nueva versión de SDL Trados Studio 2017, véase: <http://www.sdl.com/es/cxc/language/translation-productivity/trados-studio/coming-soon/ > [Fecha de consulta: 13 de noviembre de 2016].

A efectos prácticos, hemos incluido los elementos que realmente vamos a necesitar para realizar la traducción: el término y su equivalente, el número de ficha por si es necesario realizar alguna consulta adicional y una definición resumida por si el traductor necesita consultar algún tipo de ambigüedad (algunas siglas tienen varios referentes, por ejemplo, MAC).

7.1.1 Conversión con SDL Multiterm Convert

Una vez que contamos con el glosario en Excel, hemos de proceder a convertirlo en una base de datos de Multiterm 2014 (los pasos son iguales en Multiterm 2007, 2009 o 2011). Para ello, hemos de abrir el conversor SDL Multiterm Convert y seguir los pasos que nos indica el asistente a partir de la opción Formato Microsoft Excel. A continuación, ilustramos el proceso mediante una serie de capturas de pantalla que realizamos durante el mismo:

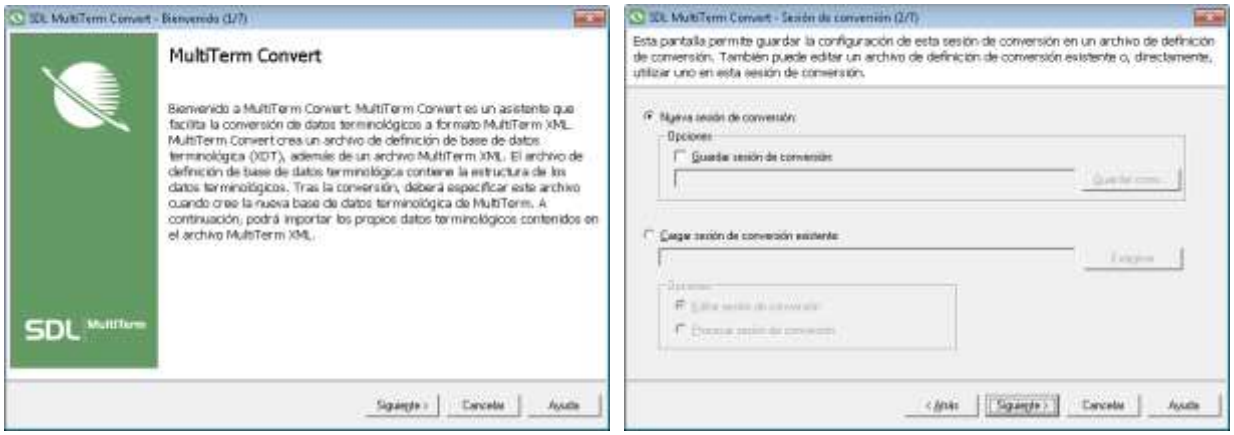


Figura 16. Primeros pasos en SDL Multiterm Convert.

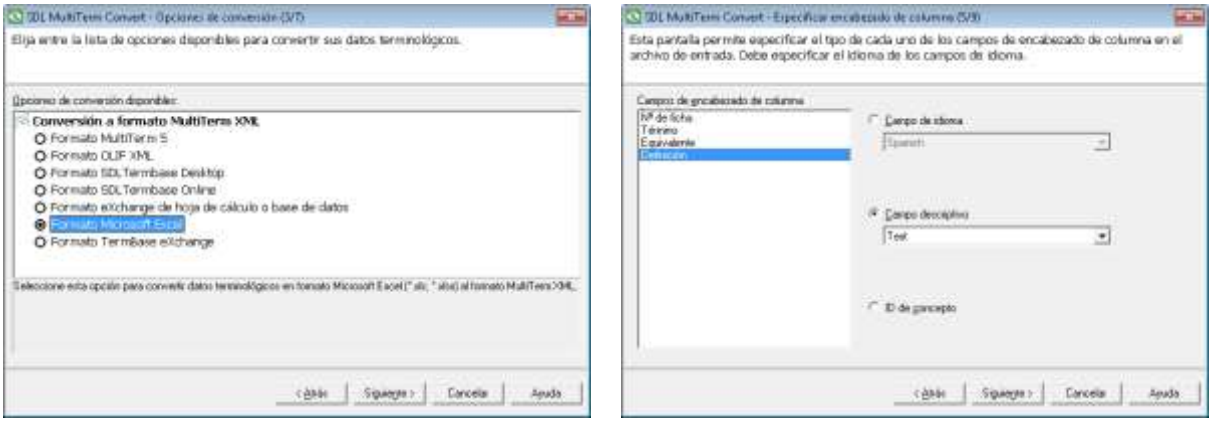


Figura 17. Configuración de la conversión a partir de un glosario en formato Excel.

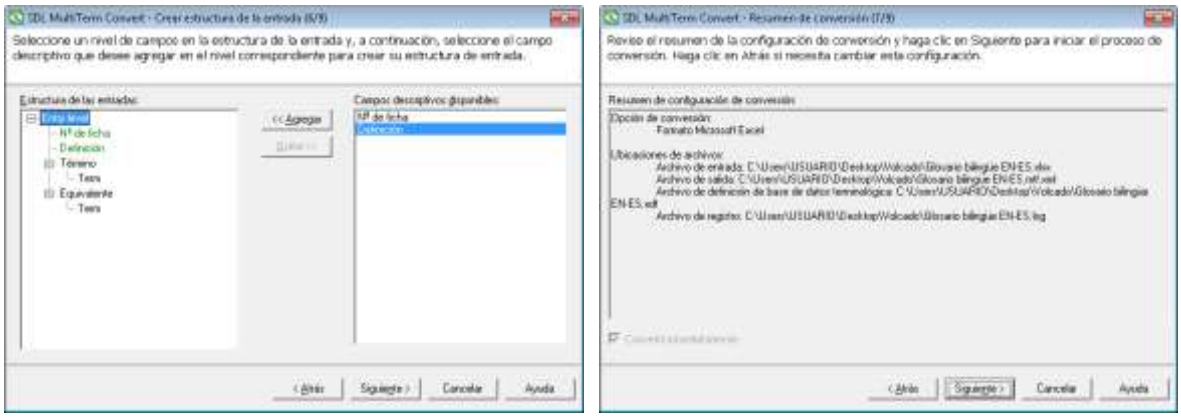


Figura 18. Último paso: selección del nivel de los campos incluidos y revisión final.

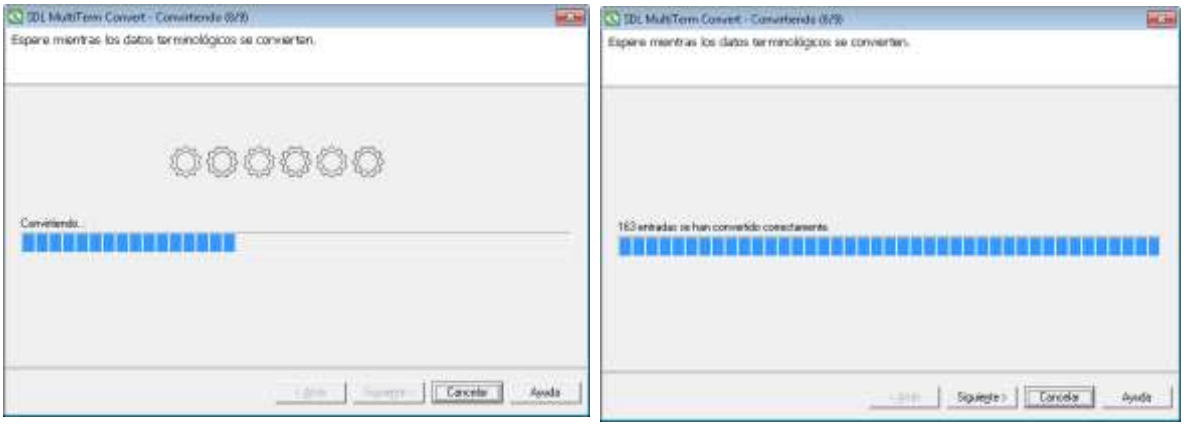


Figura 19. Duración del proceso en una base de datos terminológica de gran tamaño.

El resultado final de este proceso son los archivos .xml y .xdt en el mismo directorio que nuestro archivo Excel. Estos nos permitirán seguir con el siguiente paso, es decir, la creación de una base de datos terminológica en SDL Multiterm Desktop. Hemos utilizado la versión 2014 por ser la más actual en el momento en que se realizó este trabajo de investigación.

7.1.3 Creación de la base de datos en SDL Multiterm Desktop

El siguiente paso es abrir SDL Multiterm Desktop y crear una base de datos terminológica a la que importaremos los términos del glosario bilingüe. Para ello, hacemos clic en **Base de datos terminológica > Crear base de datos terminológica** e indicamos una ruta y un nombre para guardarla. A

continuación, seguimos los pasos del asistente y configuramos nuestra base de datos terminológica. En todo este proceso, partimos de la ubicación del archivo de definición que creamos anteriormente (**.xdt**). Para ello seleccionamos la opción **Cargar archivo de definición de base de datos terminológica existente** y cargamos nuestro archivo **.xdt**.

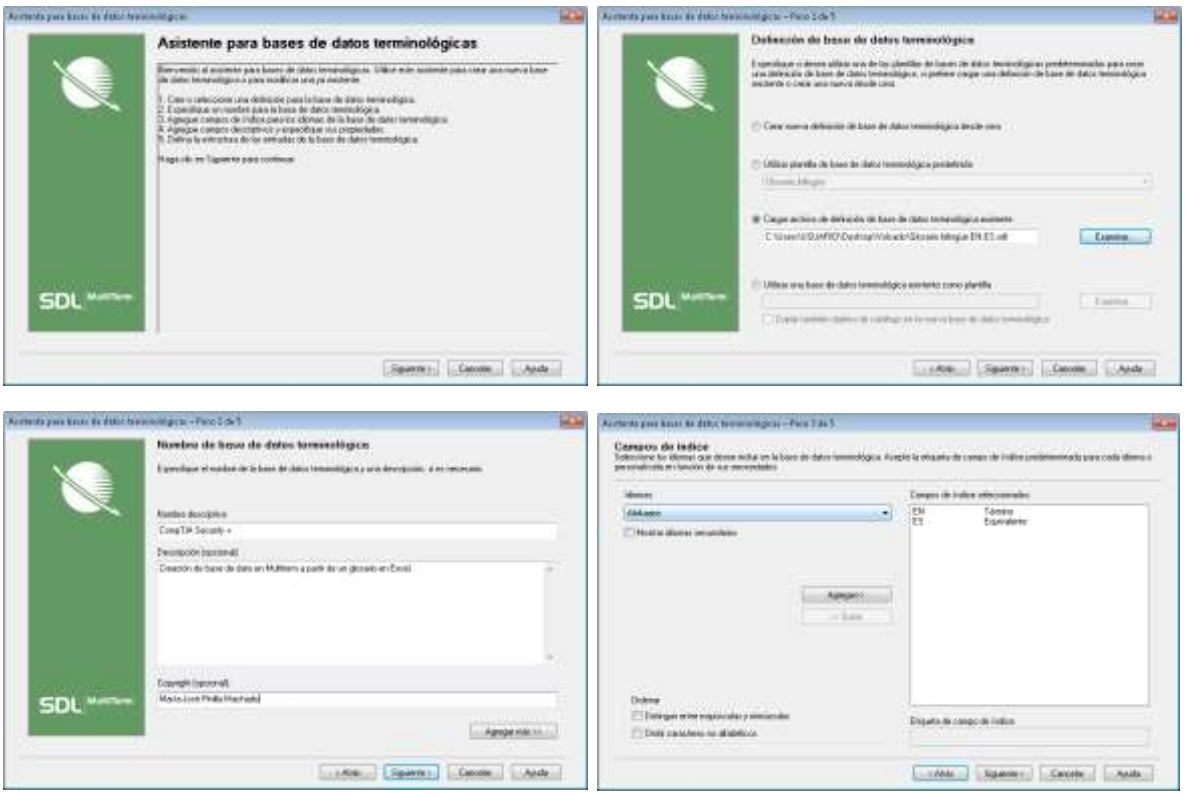


Figura 20. Proceso de creación de una base de datos terminológica en Multiterm 2014.

A continuación se procede a la creación de los campos descriptivos de la base de datos terminológica; tras ella, se realiza la revisión final y se cierra el asistente.

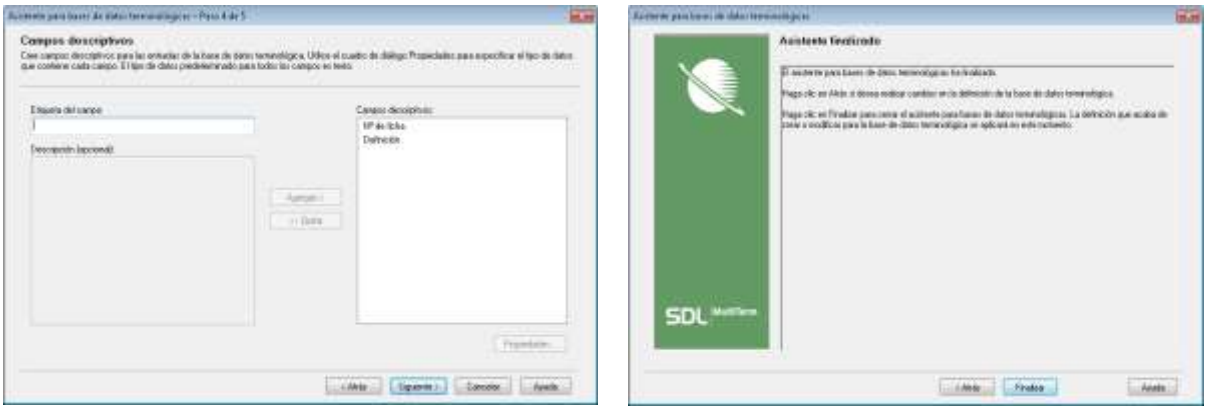


Figura 21. Creación de los campos descriptivos de la base de datos terminológica, revisión y cierre del asistente.

Llegados a este punto, solo tenemos que importar los términos. Para ello, hemos de seleccionar Catálogo (en la parte inferior izquierda del programa). A continuación, hacemos clic con el botón derecho en la opción **Import** del menú y seleccionamos Procesar. Las siguientes capturas de pantalla que realizamos durante la creación de nuestra base de datos terminológica ilustran este proceso de forma gráfica.

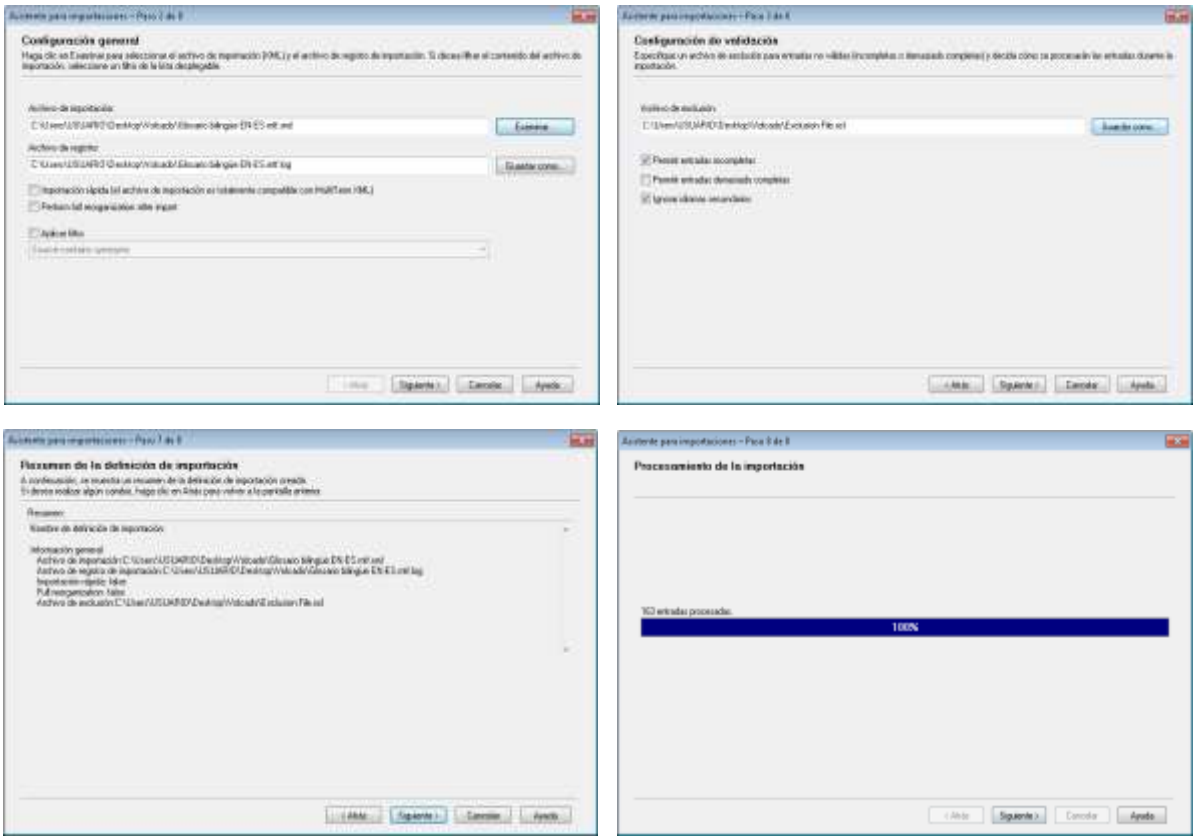


Figura 22. Proceso de importación del glosario bilingüe a una base de datos terminológica en Multiterm.

Tras este proceso, hemos creado satisfactoriamente una base de datos terminológica en Multiterm con todos los términos y las equivalencias de las fichas terminológicas que creamos con anterioridad, así como con sus definiciones. Como cabe imaginar, esto aporta numerosas ventajas al proceso de traducción y al control de la calidad de las traducciones. Al trabajar con una base de datos de Multiterm vinculada a Trados nuestro proceso de traducción será mucho más ágil, ya que el programa reconocerá los términos de cada segmento que estén incluidos en el glosario. Veamos, pues, algunos ejemplos de su aplicación práctica al día a día del traductor.

Las siguientes capturas de pantalla ilustran el resultado de la creación de nuestra base de datos terminológica en Multiterm.

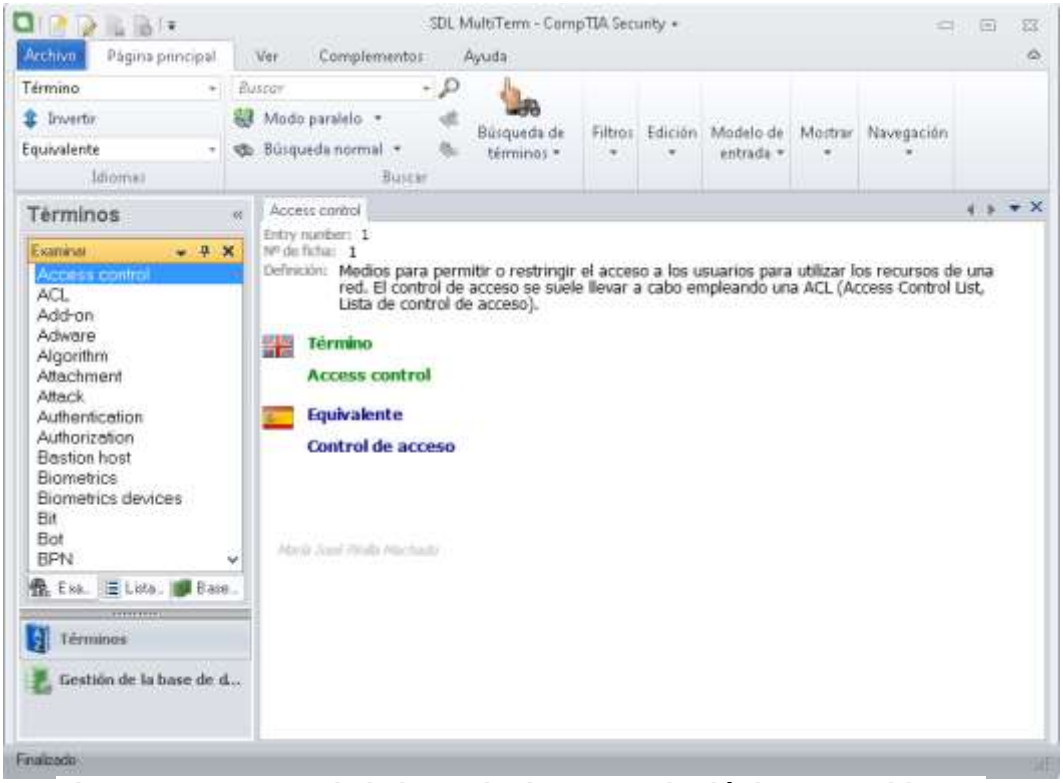


Figura 23. Muestra de la base de datos terminológica en Multiterm.

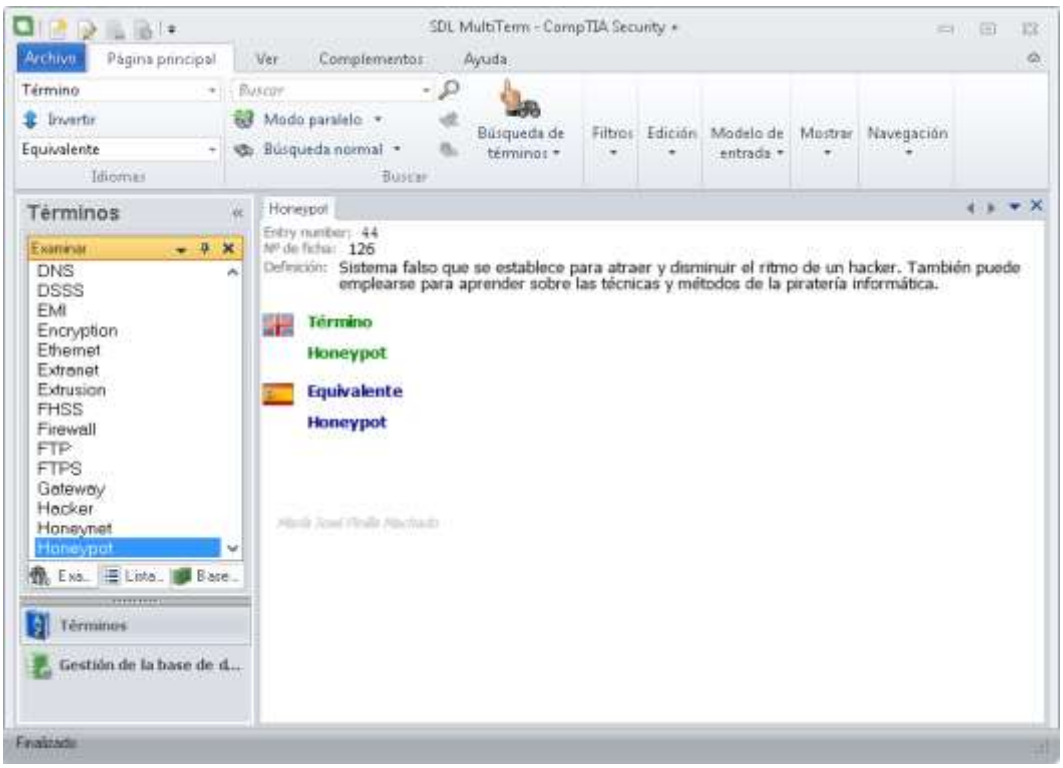


Figura 24. Muestra de la base de datos terminológica en Multiterm.

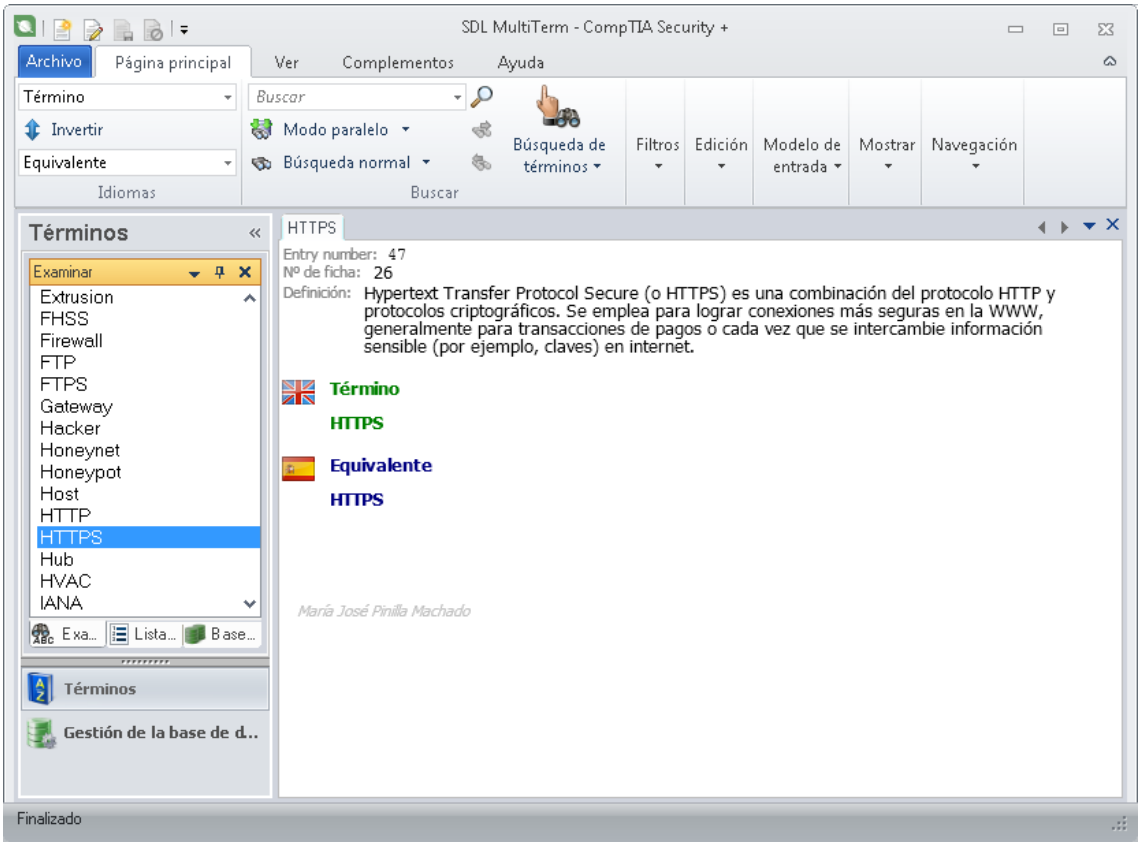


Figura 25. Muestra de la base de datos terminológica en Multiterm.

Por último, nos gustaría destacar que este proceso se puede llevar a cabo con otros formatos de archivo, por ejemplo, Multiterm 5, XML, hojas de cálculo o bases de datos, archivos .txt, etc. Por lo tanto, podemos seguir los mismos pasos con glosarios que nos proporcionen las empresas o los clientes e incluso vincularlos con los nuestros propios con el fin de optimizar el trabajo de traducción. Todo ello dependerá de las condiciones del encargo en cuestión, ya que para algunos proyectos (en especial, para los grandes proyectos de traducción especializada) ofrece más ventajas que para otros (por ejemplo, un proyecto corto con baja densidad de lenguaje especializado).

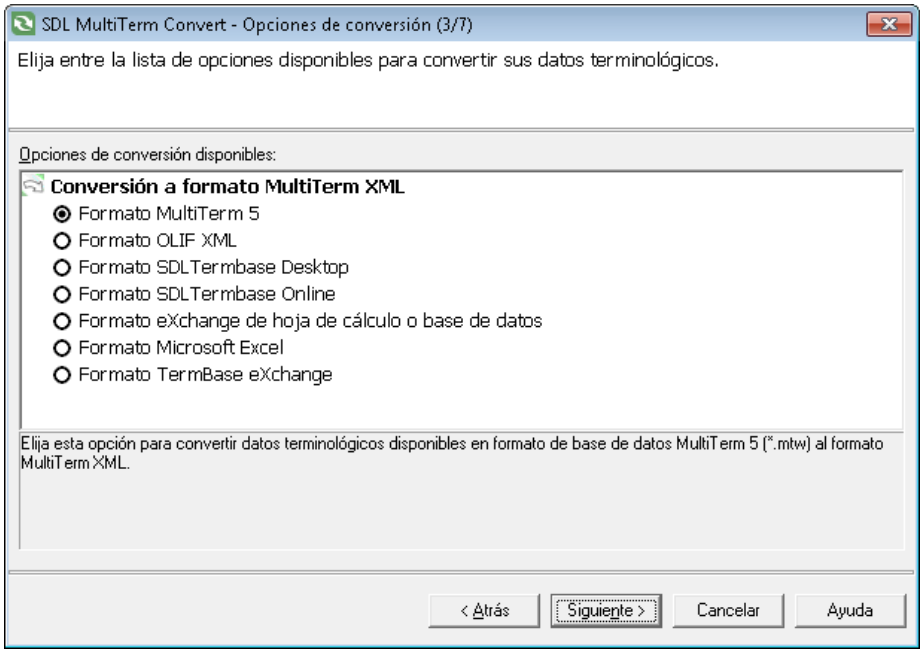


Figura 26. Tipos de archivos que admiten conversión a formato Multiterm.

7.4. Creación de un proyecto de traducción en Trados

Trados es un programa de traducción asistida en el que se pueden crear proyectos de traducción o traducir archivos individuales. En el caso de este trabajo de investigación y dado que contamos con varios archivos para traducir (uno por capítulo), lo más práctico es crear un proyecto de traducción que utilice la misma base de datos terminológica y la misma memoria de traducción.

Una **memoria de traducción**[46] es un archivo que va guardando los segmentos de texto traducidos a medida que vamos traduciendo. Esto nos permite realizar análisis de repeticiones con todo lo que ello implica. Si un segmento se repite, no tenemos que volver a traducirlo. Simplemente, el programa nos indica el porcentaje de repetición.

Para la creación de un proyecto terminológico, hay que tener en cuenta varias cuestiones. A continuación se incluyen algunas capturas de pantalla que ilustran este proceso. De no tener en cuenta dichas cuestiones, el proyecto de traducción en Trados sería infructuoso y no cumpliría su propósito. Como cabe esperar, es el traductor especializado el que debe conocer en profundidad el software informático con el que va a trabajar, ya que esto determinará el éxito del proceso.

[46] En este epígrafe nos referimos al sentido estricto de memoria de traducción como tipo de base de datos lingüística utilizada para almacenar textos en un idioma (source) y sus correspondientes traducciones a otro (target). En este caso, se trata de una memoria de traducción EN-ES. Véase:
IATEI II. Memorias de Traducción. URL: < http://www.um.es/docencia/barzana/TEI/Informatica-Aplicada-a-la-Traduccion-Memorias-de-Traduccion.html> [Fecha de consulta: 21 de diciembre, 2016]

Para crear un proyecto de traducción en Trados (en nuestro caso en Trados 2014), en primer lugar, hemos de determinar los detalles del mismo, es decir, el nombre, una descripción (muy útil cuando trabajamos con múltiples proyectos y a efectos de archivo) y la ubicación. Un proyecto de traducción necesita una carpeta vacía, ya que está compuesto de varios archivos.

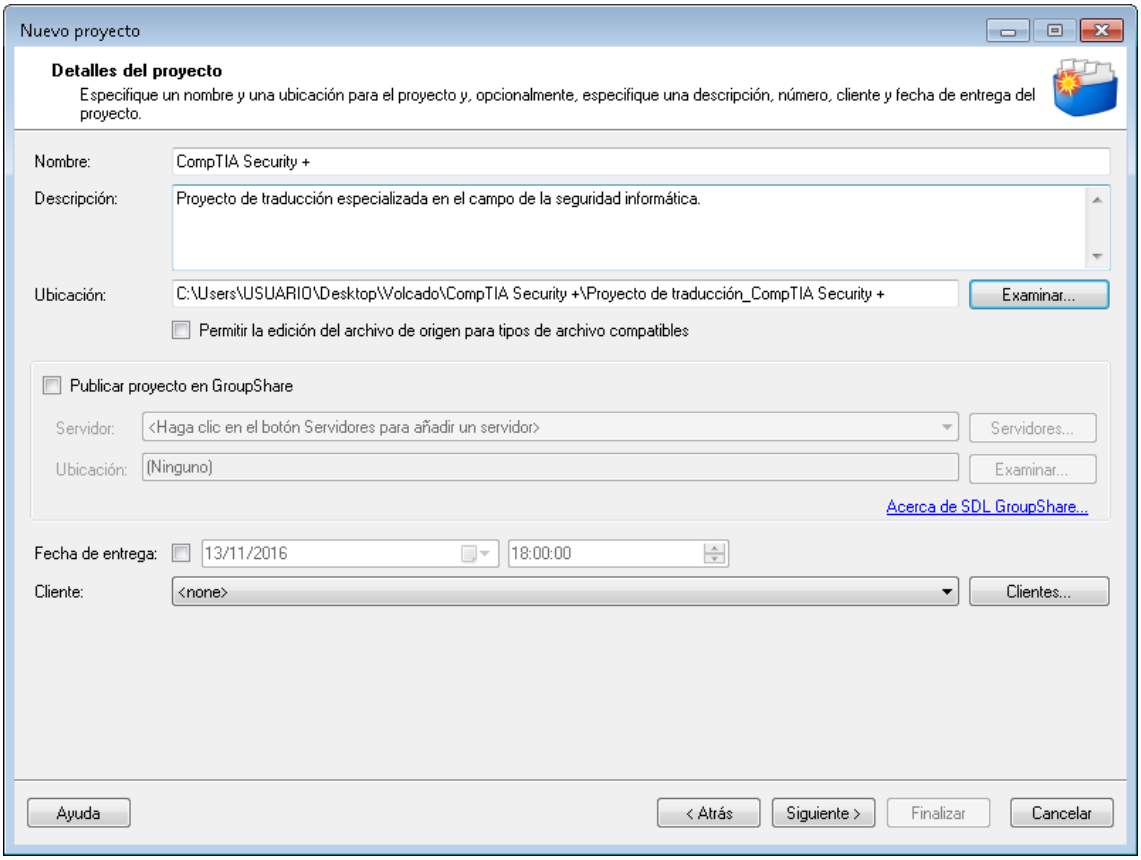


Figura 27. Primeros pasos de la creación de un proyecto de traducción en Trados.

A continuación, hemos de especificar el idioma original y el idioma de destino. Esta especificación determinará las memorias de traducción que podemos elegir. En este caso, partiremos de una nueva memoria de traducción. Como podemos observar en la siguiente captura de pantalla, Trados ofrece muchas combinaciones de idiomas posibles. Nosotros trabajamos con un proyecto de inglés americano a español de España: EN (United States) a ES (Spain).

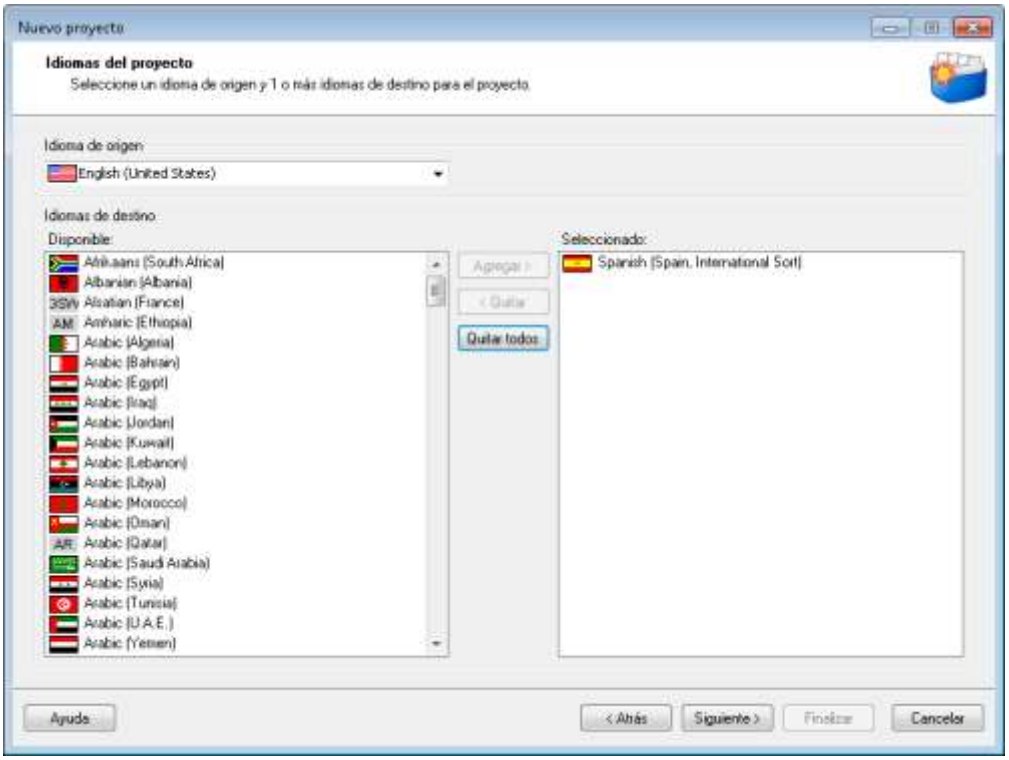


Figura 28. Especificación del idioma del proyecto de traducción.

El siguiente paso del proceso es añadir los archivos que vamos a traducir utilizando la misma memoria de traducción y la misma base de datos terminológica. En aras de la brevedad, hemos incluido los cinco capítulos seleccionados para ilustrar este proceso. Como hemos mencionado con anterioridad, Trados también ofrece la posibilidad de traducir un documento individual, pero el procedimiento que se seguiría es distinto.

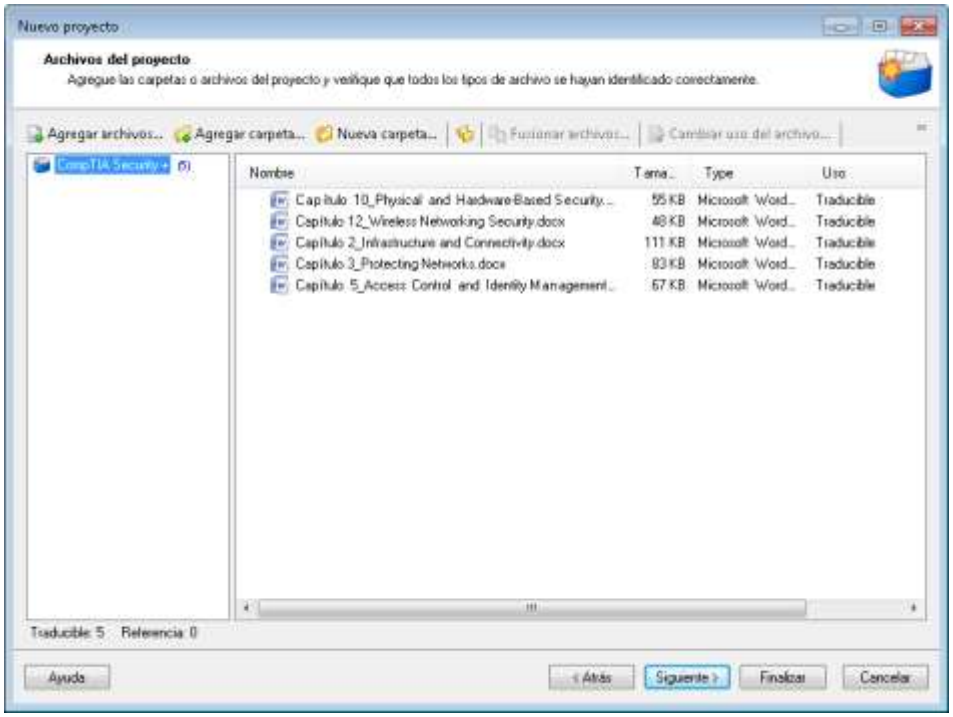


Figura 29. Adición de archivos al proyecto de traducción.

A continuación, es el momento de añadir la memoria de traducción. En este caso, tenemos dos opciones. Por un lado, podemos utilizar una memoria existente que ya tengamos de otros proyectos relacionados o que nos haya proporcionado la agencia de traducción con el fin de ahorrar costes. Por otro lado, podemos crear una memoria de traducción nueva específica para este proyecto (como en nuestro caso) con el fin de ir archivando los segmentos traducidos mientras vamos trabajando. Esto nos lleva a traducir mayor contenido, entregar un texto de mayor coherencia y aumenta nuestra productividad como traductores. Como resulta evidente, al trabajar así la calidad aumenta de forma exponencial.

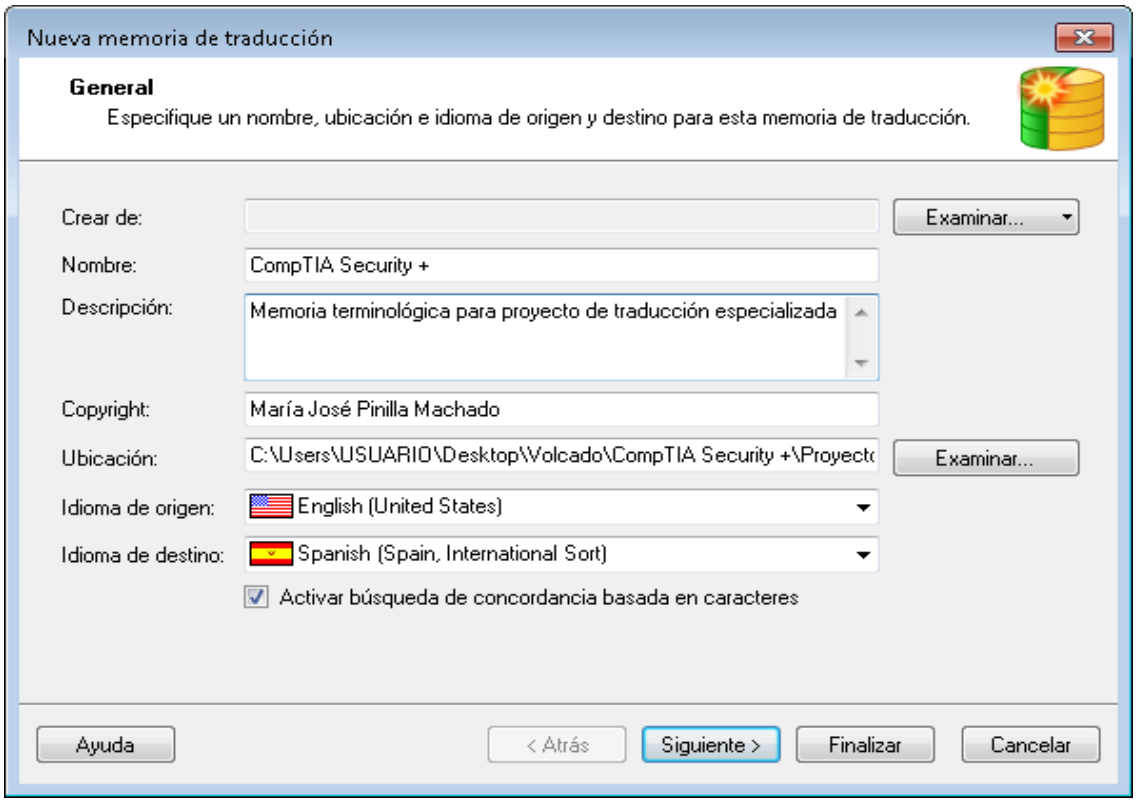


Figura 30. Configuración de una nueva memoria de traducción.

La creación de una memoria de traducción es un proceso laborioso que lleva un amplio margen de tiempo.

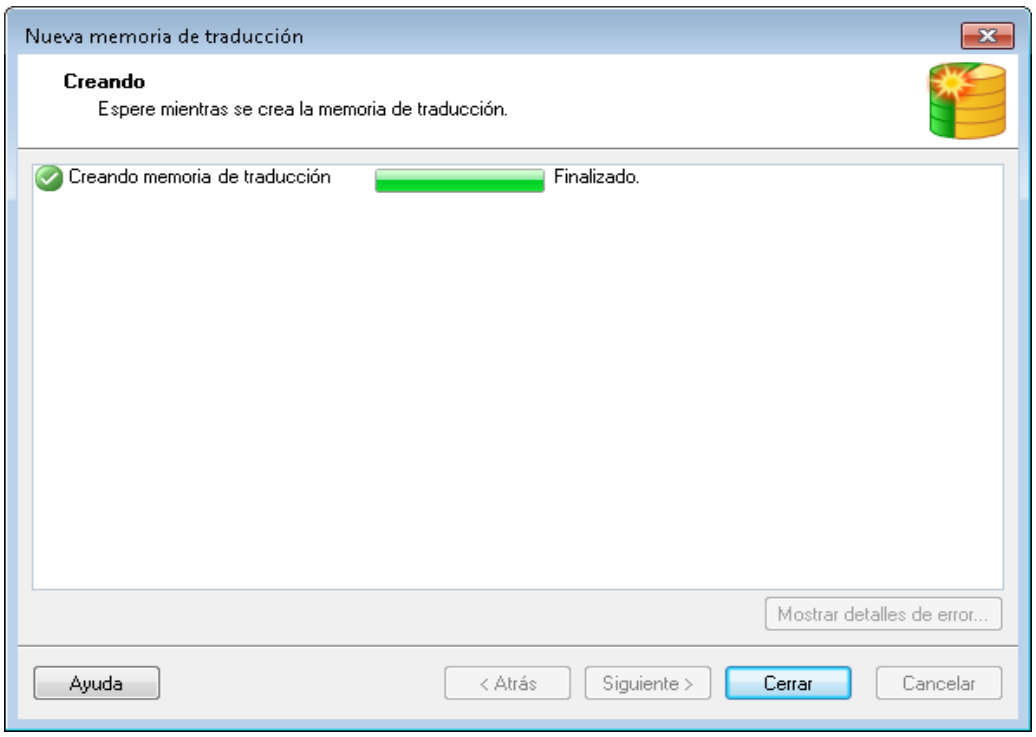


Figura 31. Creación de la memoria de traducción.

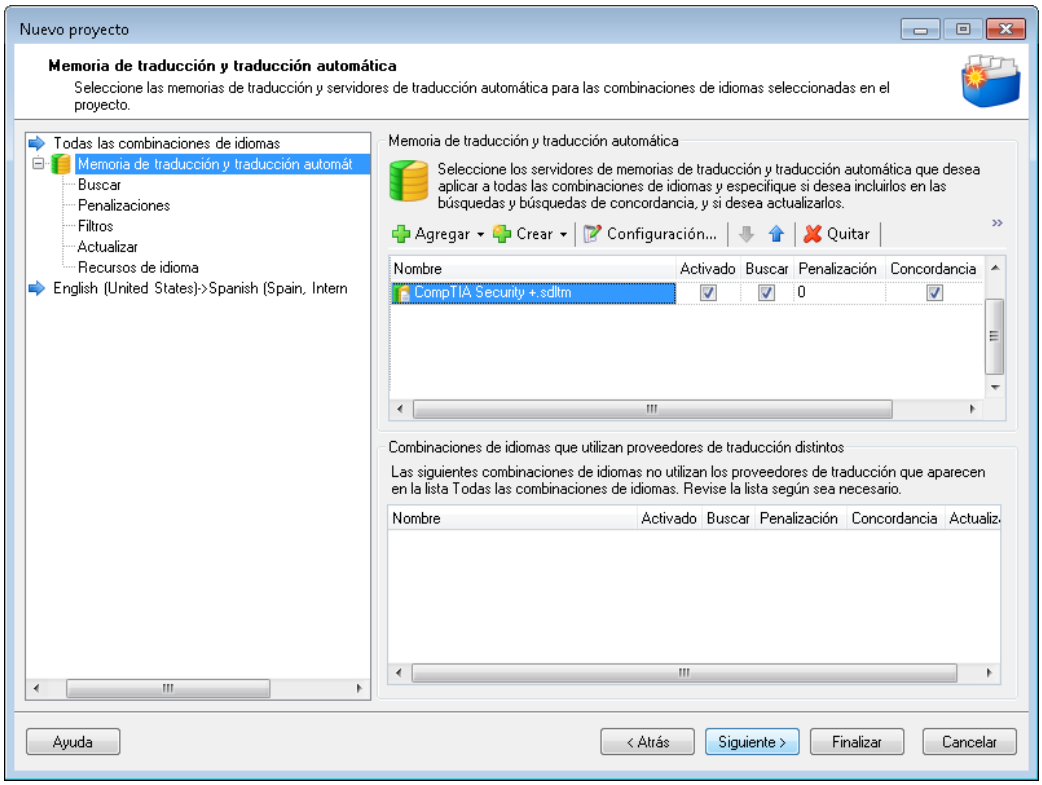


Figura 32. Incorporación de la memoria de traducción al proyecto.

Agregar la memoria de traducción al proyecto es fundamental, ya que de lo contrario traduciremos sin que se archiven los segmentos traducidos y, por lo tanto, no conseguiremos el objetivo deseado, que no es otro que optimizar el proceso de traducción con el fin de obtener una mayor calidad.

El siguiente paso es añadir la base de datos terminológica, que se explica en el siguiente epígrafe.

7.5 Vinculación de una base de datos terminológica a Trados

En un epígrafe anterior creamos la base de datos terminológica a partir de las fichas del proyecto terminológico de nuestro trabajo de investigación. Como es lógico, durante el proceso de traducción podemos consultarlas sin problema y de forma ágil sin perder mucho tiempo. Solo tenemos que tener abierta la base de datos terminológica mientras trabajamos. Sin embargo, aún podemos dar un paso en la optimización de nuestro trabajo como traductores especializados.

Si seguimos los pasos de la creación del proyecto terminológico, observamos que, una vez agregada la memoria de traducción, el asistente también nos permite vincular una base de datos terminológica a nuestro proyecto. Es aquí donde vinculamos el trabajo realizado anteriormente en Multiterm a Trados tal y como muestra la siguiente captura de pantalla.

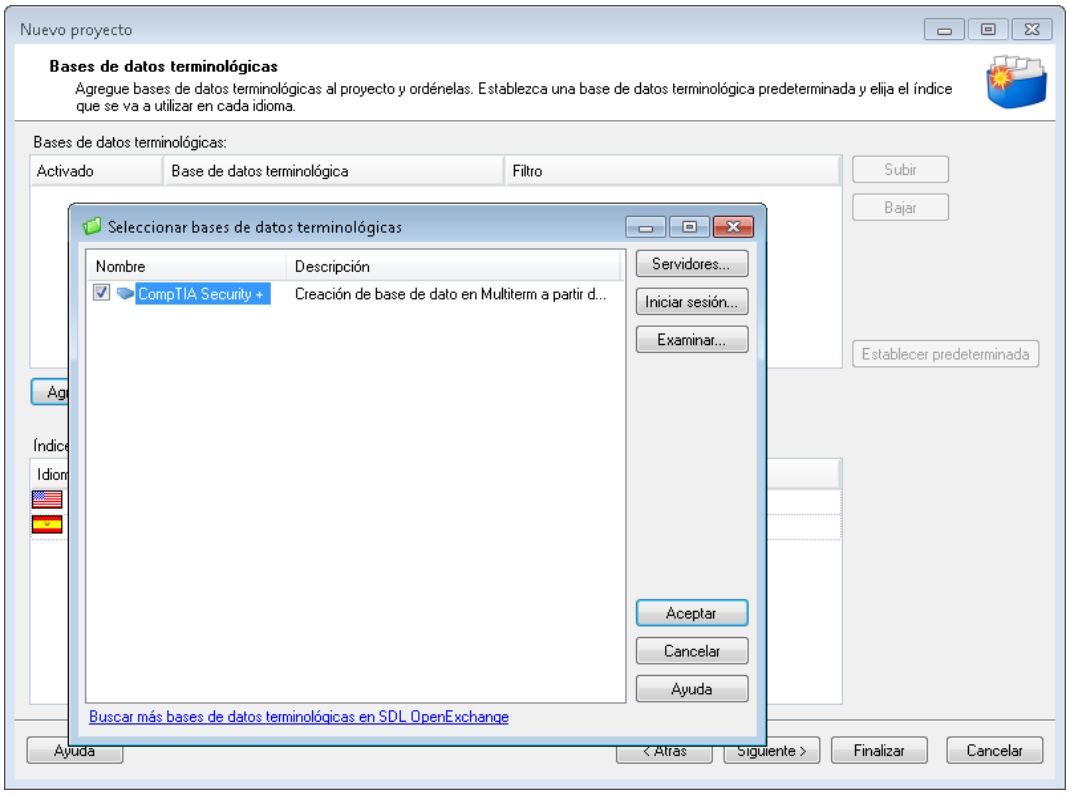


Figura 33. Selección de una base de datos terminológica para un proyecto de traducción.

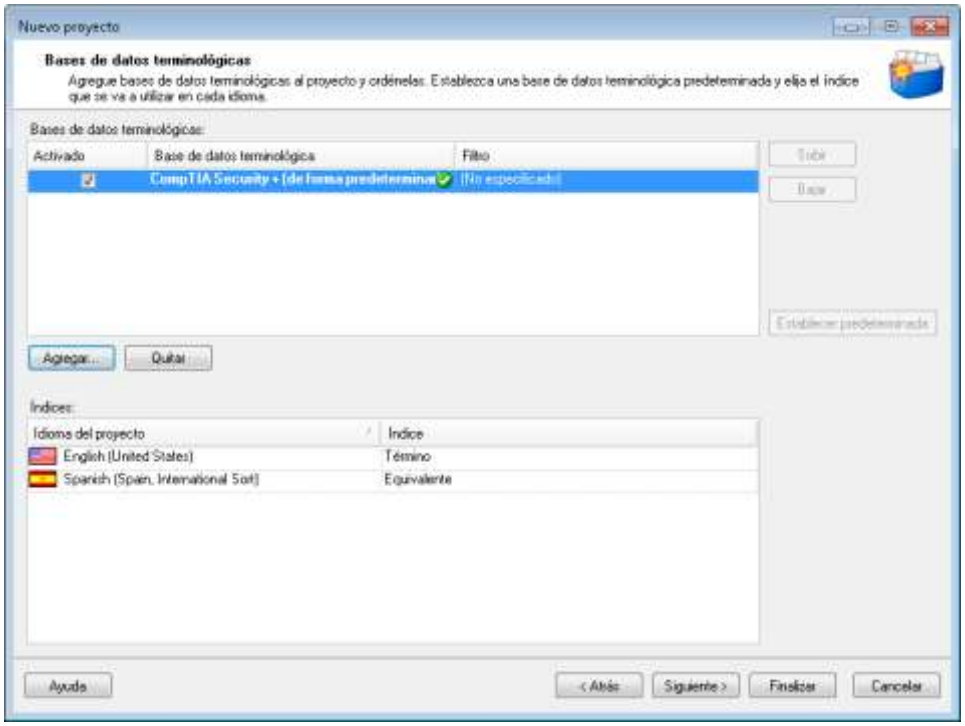


Figura 34. Incorporación de una base de datos terminológica a un proyecto de traducción.

Una vez creada la memoria de traducción y agregada la base de datos terminológica, el asistente de creación del proyecto nos ofrece un resumen con los detalles del mismo para que podamos revisar que todas las especificaciones son correctas.

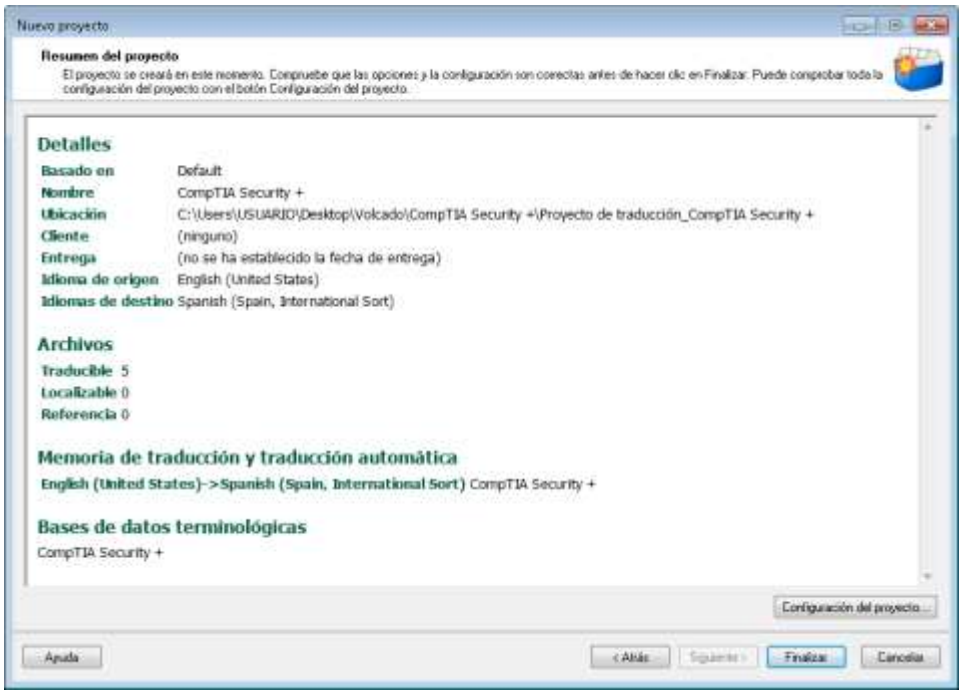


Figura 35. Detalles de un proyecto de traducción.

Como podemos observar en la captura de pantalla anterior, hemos creado un proyecto de traducción llamado *CompTIA Security +* redactado originalmente en inglés y que vamos a traducir a español. Nuestro proyecto contiene cinco archivos, es decir, los cinco capítulos seleccionados para el presente trabajo de investigación. Se ha creado una memoria de traducción EN-ES llamada *CompTIA Security +* y se ha seleccionado una base de datos terminológica con el nombre de *CompTIA Security +.*

El último paso es permitir al asistente que cree el proyecto. Para ello, se creará una carpeta con varios tipos de archivos que permitirán guardar todo el trabajo, así como la memoria de traducción.

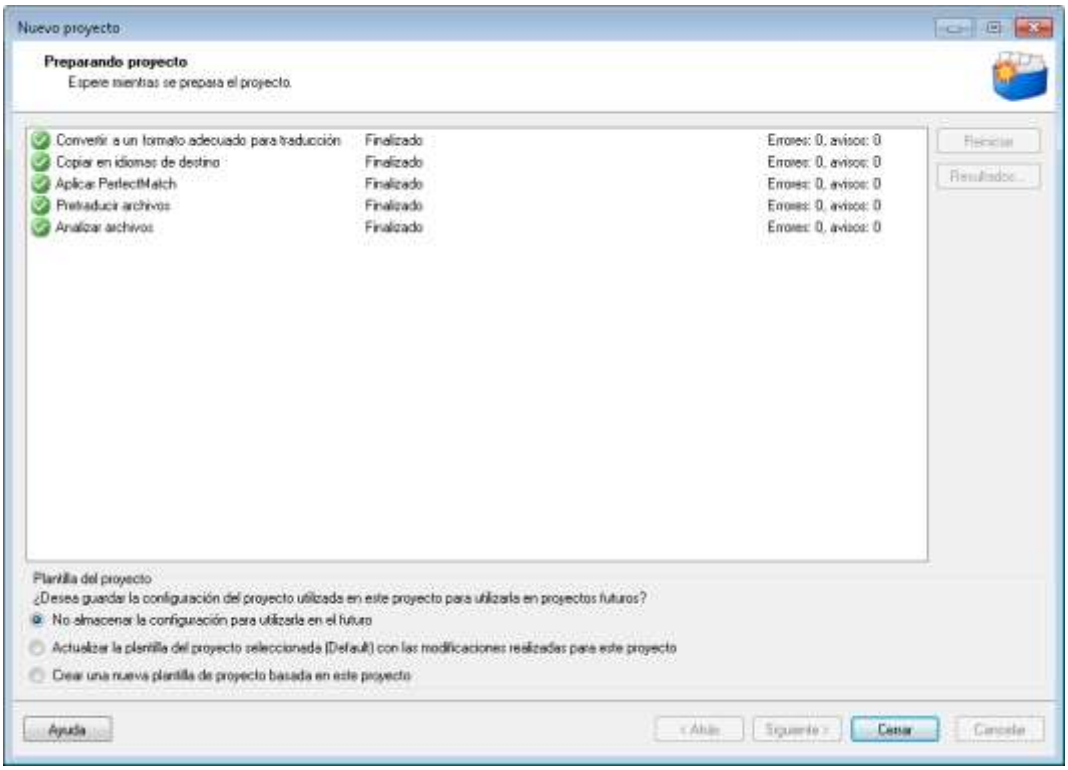


Figura 36. Finalización satisfactoria del proyecto de traducción.

7.6. Ejemplos de traducción con Trados+Multiterm

En este epígrafe mostramos algunos ejemplos de cómo se trabaja en Trados a partir de un proyecto terminológico. La siguiente captura de pantalla ilustra el punto de partida del trabajo. Este programa de traducción asistida nos muestra en todo momento el porcentaje traducido de cada archivo, lo que permite organizar el trabajo con facilidad y llevar un control del progreso del trabajo en todo momento. Además, durante el transcurso del proyecto podemos realizar distintas tareas de configuración para seguir optimizando el trabajo según las necesidades que vayan surgiendo, por ejemplo, realizar un análisis del porcentaje de repeticiones para calcular plazos o añadir nuevos términos a nuestra base de datos terminológica en caso de que sea necesario.

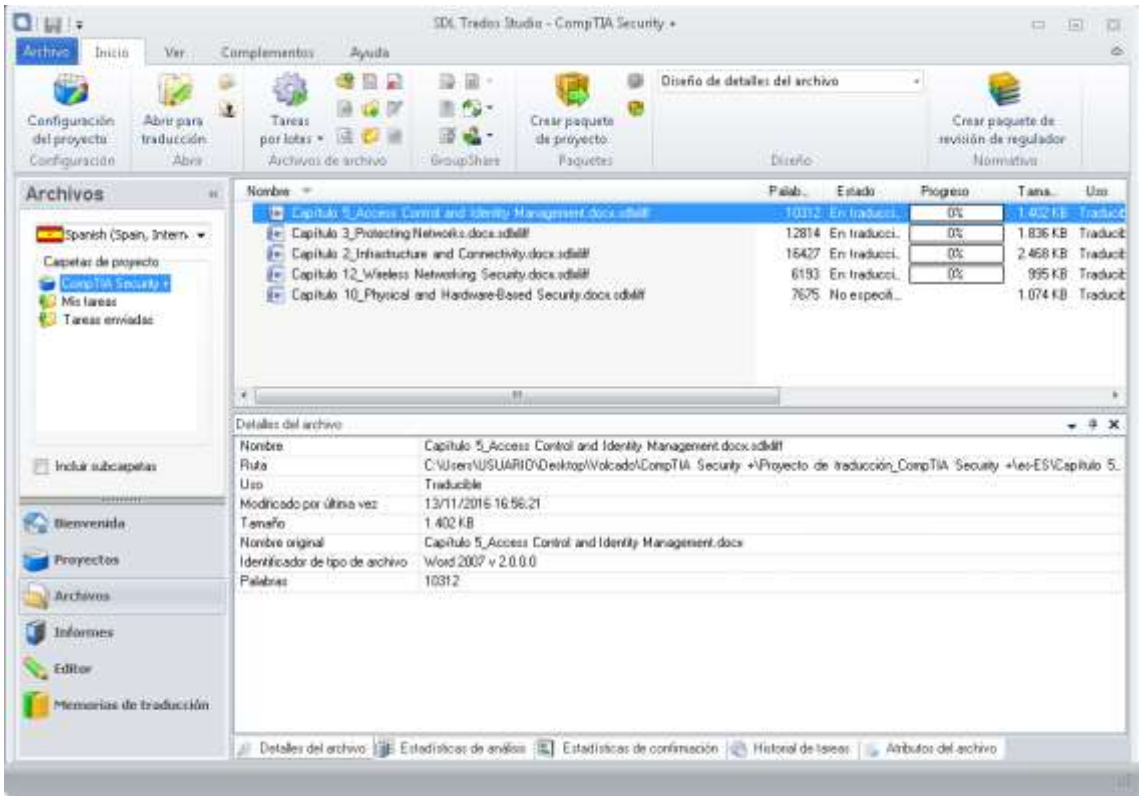


Figura 37. Punto de partida de un proyecto de traducción.

Las dos capturas de pantalla que aparecen a continuación ilustran de forma gráfica uno de los objetivos más importantes del presente trabajo de investigación, ya que en ella podemos ver cómo Multiterm y Trados se vinculan de forma que, cada vez que aparece un término de la base de datos terminológica en los archivos objeto de traducción en Trados, este aparece

marcado en rojo para hacernos ver que se trata de un término que ya tiene una traducción establecida. Es más, una vez que empezamos a escribir nuestra opción para dicho término, el propio programa nos muestra de forma predeterminada la opción que figura en la base de datos terminológica. Como vemos, la agilidad aumenta de forma exponencial al trabajar así, ya que esto ocurrirá de forma sistematizada cada vez que aparezca un término de nuestra base de datos terminológica. Por lo tanto, no tendremos que realizar más búsquedas documentales sobre estos términos, ni tampoco detenernos a pensar cómo los vamos a traducir, ni cómo los hemos traducido si es que ya han aparecido en el texto con anterioridad.

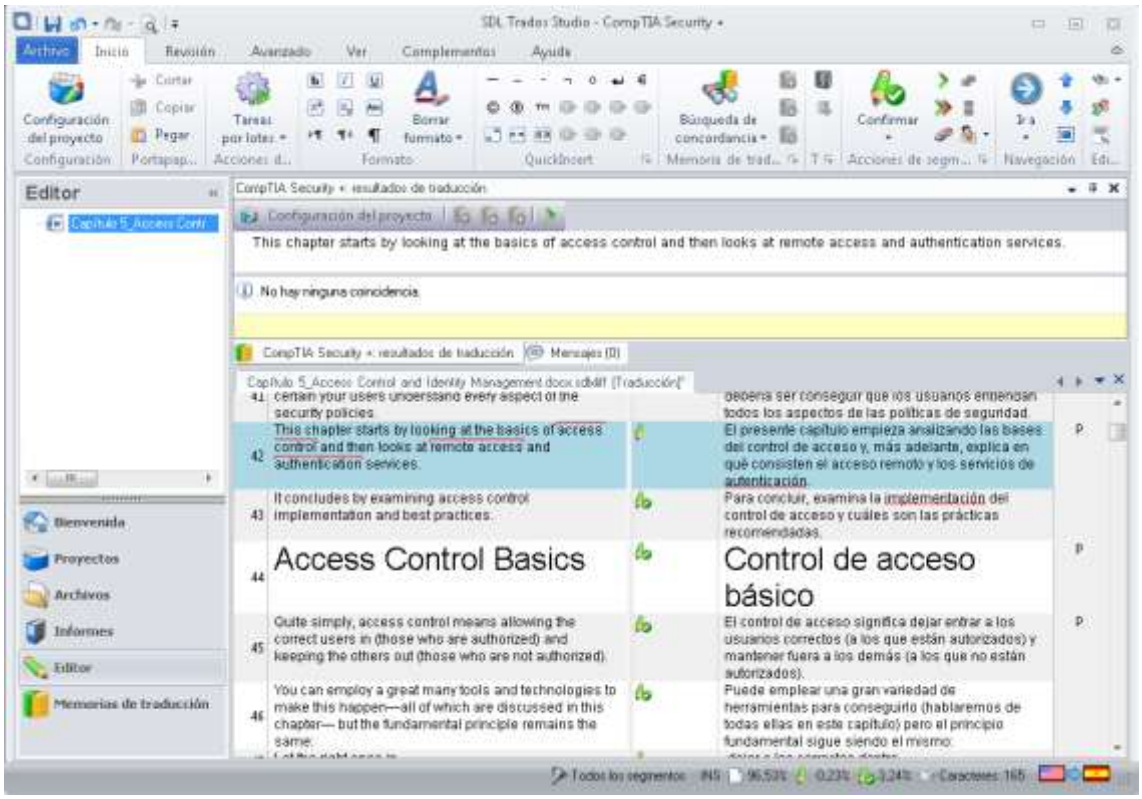


Figura 38. Ejemplo de traducción con base de datos incorporada a Trados.

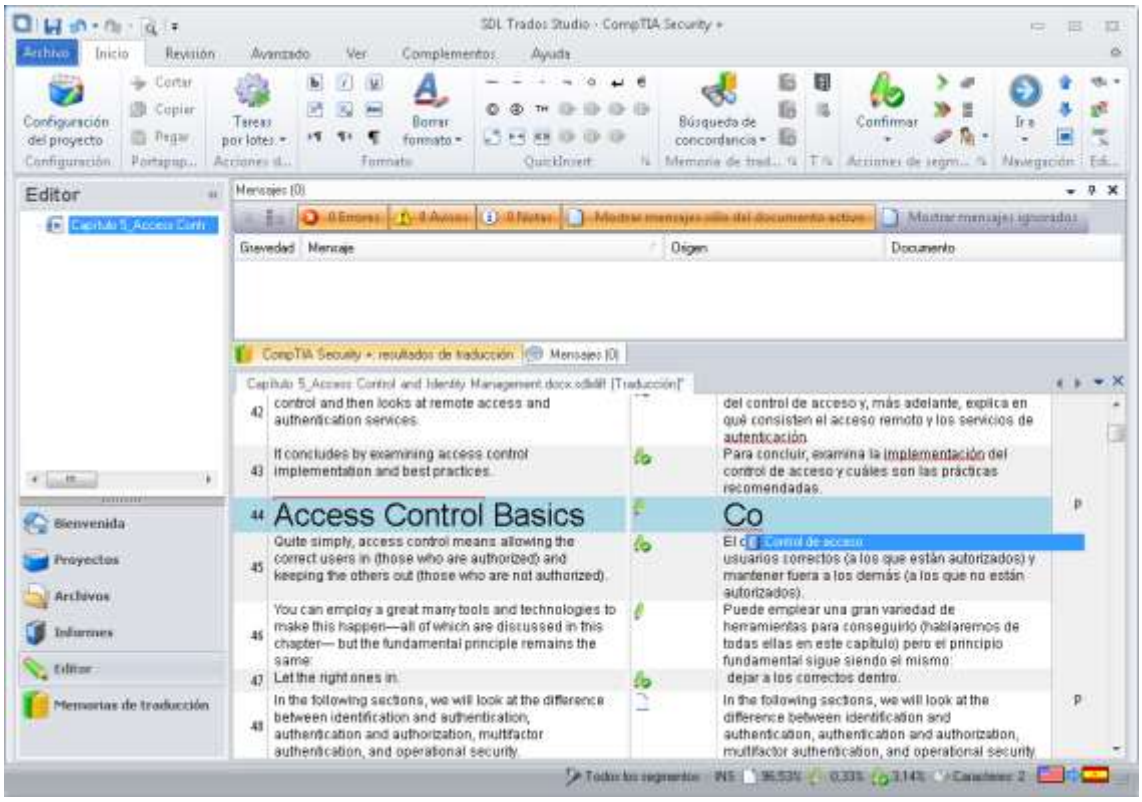


Figura 39. Ejemplo de traducción con base de datos incorporada a Trados.

8. RESULTADOS

A partir del análisis de la traducción de un manual de 650 páginas sobre seguridad informática llevada a cabo en 2011 por la misma persona que ha realizado este trabajo de investigación, el presente proyecto se centra en las nociones básicas de la disciplina terminológica y las características de los textos especializados, más concretamente de los textos científico-técnicos. Además, al tratarse de un texto híbrido con matices claramente didácticos, se describen las características de los textos didácticos, así como de los manuales técnicos y la seguridad informática. Dada la extensión del manual traducido, se seleccionaron dos capítulos representativos y, para respaldar la traducción, elaboramos un glosario bilingüe y un fichero terminológico con 165 fichas que se han convertido en el principio de una base de datos que podría resultar realmente útil tanto como para traductores especializados, como para estudiantes de traducción.

Hemos obtenido los siguientes resultados que corroboran nuestros objetivos e hipótesis iniciales:

- **Análisis de un encargo de traducción:** Como cabe esperar, la realización de un proyecto de traducción no se encuentra aislada y fuera de contexto. Antes de abordar la tarea de traducción propiamente dicha, el traductor especializado debe conocer las particularidades del encargo. En este caso, no solo nos referimos a los plazos, el presupuesto o el formato de entrega, que, por otra parte, son fundamentales, sino que, además, hemos de tener en cuenta si el texto se va a publicar o no, conocer en profundidad las recomendaciones de estilo y formato que emplea la agencia con la que vamos a colaborar, a quién se dirige nuestra traducción y conocer el software o las aplicaciones informáticas con las que vamos a trabajar, entre otras muchas cuestiones. Todos estos elementos determinantes del proyecto de traducción condicionarán el trabajo del traductor profesional, así como la metodología y las fases que seguir.

- **Identificación de las características fundamentales de un texto técnico:** Conocer las características de los textos técnicos y aplicar estos conocimientos con el fin de identificar los rasgos propios del corpus

elegido, tanto en el nivel morfológico como en el nivel léxico-semántico, permite analizar de forma correcta su tipología y naturaleza para trasladar los rasgos identificados a la lengua española de modo adecuado. Gracias a este análisis, llegamos a la conclusión de que el manual seleccionado era un ejemplo claro de texto técnico, pero, además, presentaba rasgos claros de otra tipología textual bien definida, el texto didáctico.

- **Identificación de las características fundamentales de un texto didáctico:** Del mismo modo, conocer las características de los textos didácticos y aplicar estos conocimientos para identificar las características presentes en el corpus objeto de análisis o traducción permite identificar su tipología y reflejar de modo adecuado los rasgos pertinentes en la lengua meta. Nuestro análisis determinó que el manual seleccionado, además de presentar rasgos de los textos científico-técnicos, era un ejemplo claro de texto didáctico; por lo tanto, nos encontramos ante un texto de naturaleza híbrida.

- **Identificación de las características fundamentales de un texto híbrido:** Como demuestra este manual, los textos no siempre se limitan a presentar las características de una única tipología textual, sino que tienen rasgos distintivos de varias tipologías con el fin de atender a distintos propósitos. Por un lado, el manual seleccionado es claramente un texto técnico centrado en el tema de la seguridad informática, en el que aparecen elementos representativos de este tipo de textos como, por ejemplo, claridad, precisión, verificabilidad, universalidad y objetividad que han de trasladarse a la versión traducida del texto. Pero, por otro lado, también encontramos en él características plenamente distintivas de los textos didácticos. Por ejemplo, podríamos afirmar sin lugar a dudas que el manual seleccionado es un instrumento, una herramienta de trabajo que permite un proceso de construcción y desconstrucción de un universo comunicativo en el que los receptores tienen la posibilidad de asumir otro papel más allá del de reproductores del emisor, es decir, a partir de una serie de instrumentos de base (los capítulos del manual) los lectores pueden comprender, reflexionar, analizar, asimilar y disentir acerca de la realidad cognitiva que se les ofrece. En este caso, además, el manual les permite prepararse un examen para obtener una titulación específica de seguridad informática.

- **Constatación de la importancia de un análisis terminológico para la traducción:** Uno de los primeros pasos seguidos en nuestro proyecto fue repasar las bases teóricas de la terminología y aplicar estos conocimientos terminológicos a la traducción. Sin lugar a dudas, esto constituye una etapa esencial previa a la traducción de un texto especializado que nos permite descubrir la naturaleza y la densidad terminológica del texto con el que estamos trabajando. Si tenemos en cuenta que el primer paso para realizar la traducción de un texto con éxito es comprenderlo, es vital establecer las relaciones semánticas entre los términos y el texto del que forman parte. No obstante, cabe destacar que, con la práctica y la experiencia, el traductor profesional va automatizando paulatinamente estas destrezas y habilidades.

  Conocer las bases teóricas de la terminología permite al traductor el acceso a herramientas realmente útiles como son los sistemas de conceptos que posibilitan una comprensión visual y completa del texto, los **glosarios bilingües,** que facilitan la homogeneización en un lenguaje que está en continuo cambio y evolución como es el lenguaje de la seguridad informática y, por último, las fichas terminológicas, que, además de servir a los propósitos citados con anterioridad, pueden erigirse como punto de partida de una base de datos terminológica centrada en el ámbito de análisis.

- **Análisis de la terminología del ámbito de la seguridad informática:** El manual analizado reúne una extensa y detallada recopilación de información relacionada con la seguridad informática que incluye medidas técnicas, cálculos del riesgo, temas de infraestructura y conectividad, protección de redes, amenazas y vulnerabilidades, control de acceso y gestión de identidad, educación y protección del usuario, sistema operativo y seguridad de aplicación, fundamentos e implementación de la criptografía (Ramió Aguirre, 2006), seguridad física y basada en hardware, seguridad y vulnerabilidad en la red, seguridad de red inalámbrica, recuperación de desastres y respuesta a incidentes, directivas y procedimientos relacionados con la seguridad y administración de seguridad.

  Contextualizar el manual dentro del ámbito de la seguridad informática resulta esencial por numerosos motivos: identificación de la terminología del corpus, análisis de la tipología textual, traslado de las estructuras

adecuadas de este tipo de texto al español, etc. Todo ello ha resultado evidente en los distintos apartados de este manual. Pero, además, el análisis efectuado nos ha llevado a nuevas conclusiones. Una de las más relevantes es, sin lugar a dudas, la importancia de una homogeneización terminológica en este ámbito para producir traducciones de calidad y evitar crear confusión y ambigüedades entre los receptores, que suelen ser profesionales del sector. Sin la ayuda de la Terminología y las herramientas que esta nos proporciona no podría conseguirse. Es así como surge la idea de la **creación de una base de datos terminológica centrada en la seguridad informática**, elaborada a partir de las fichas terminológicas que se incluyen en este trabajo de investigación, con el fin de ponerla a disposición de traductores profesionales y estudiantes de traducción.

Se han elaborado 165 fichas terminológicas, de las cuales 25 pertenecen a términos que son neologismos, 30 son préstamos y calcos, 65 son siglas y acrónimos y 45 son traducciones por equivalencia.

Al extraer los porcentajes de esta terminología, un 15,15% son neologismos, un 18,18% son préstamos y calcos, un 39,40% son siglas y acrónimos, y un 27,27% son traducciones por equivalencia. Este análisis nos ayuda a cuantificar la densidad terminológica y a observar las estrategias de traducción más recurrentes en la traducción de esta área del conocimiento que es la seguridad informática. El siguiente gráfico resume esta información de forma más visual.

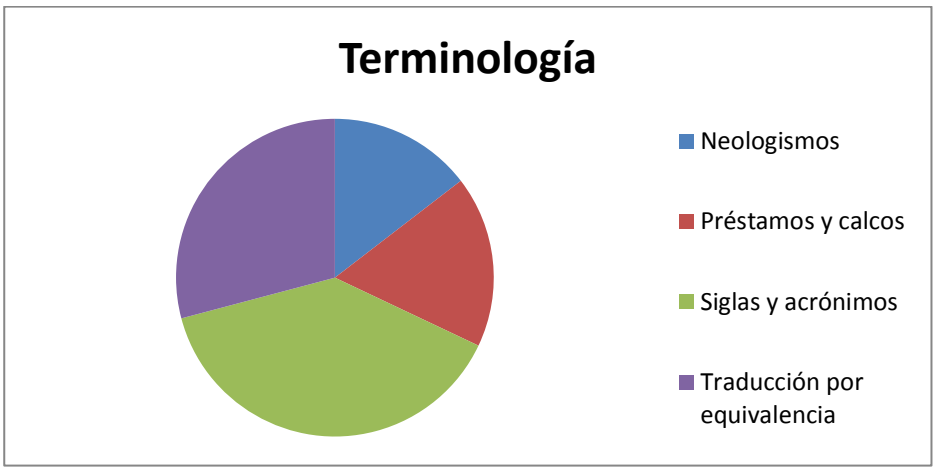


Gráfico 2. Porcentaje gráfico del texto analizado.

- **Realización de un fichero terminológico:** El fichero terminológico está formado **por 165 términos** o fraseologías que incluyen la equivalencia en castellano de cada uno de los términos seleccionados, la fuente de donde se ha extraído la equivalencia, su definición en castellano, la fuente de donde se ha extraído la definición, y en su caso, observaciones que se han de tener en cuenta por los usuarios. El número de términos es reflejo de la complejidad y grado de especialización del manual. No obstante, solo es una muestra representativa de la densidad terminológica que podemos encontrar en él. Esto es lo que nos lleva a plantear el próximo desarrollo de una base de datos más extensa a partir de este fichero terminológico.

- **Realización de un glosario bilingüe:** A partir del fichero terminológico elaboramos un glosario bilingüe de 165 términos especializados representativos del campo de la seguridad informática. Al igual que en caso anterior esto es solo una muestra representativa de la densidad terminológica que podemos encontrar en él y nos anima a profundizar en la elaboración del proyecto terminológico.

- **Elaboración de un sistema conceptual de los términos:** Tras el análisis terminológico, se organizaron conceptualmente dos de los capítulos del manual mediante un sistema de conceptos. Esto nos permitió establecer relaciones entre conceptos, ideas y términos, que describen difíciles procesos técnicos. Para aclarar el significado de los términos, recurrimos a numerosas fuentes documentales y a especialistas. Cabe destacar, además, la utilidad del propio glosario en inglés que incorpora la versión original del manual que también se tradujo al español.

- **Optimización del proceso de traducción:** Una vez que obtuvimos las fichas terminológicas y el glosario, procedimos a la exportación de los datos obtenidos a programas informáticos para la traducción asistida (Trados) y la gestión terminológica (Multiterm). Esto nos permitió sistematizar todo el trabajo terminológico y convertirlo en una herramienta útil y práctica para la práctica cotidiana del traductor especializado. Para realizar todas estas tareas de gestión terminológica el traductor debe contar con unas competencias que le habiliten para ello. No sólo nos referimos a competencias propiamente lingüísticas, también destacamos las competencias de terminología y gestión terminológica, conocimientos

especializados sobre la informática y las nuevas tecnologías aplicadas a la traducción. De este modo, pudimos demostrar que la traducción especializada se erige como una actividad compleja claramente holística, ya que en ella intervienen multitud de competencias interdisciplinares que debe reunir el traductor especializado.

- **Reflexión y análisis de la experiencia propia como traductora:** La elaboración de este trabajo de investigación tras cinco años como traductora profesional ha sido una experiencia realmente enriquecedora y productiva, ya que ha permitido a esta autora teorizar sobre su actividad profesional, analizarla, desglosarla y descomponerla hasta su mínimo exponente. Además, han surgido retos e ideas para seguir desarrollando e investigando en un futuro, como es la ampliación del fichero terminológico. La importancia de la Terminología y la utilidad de las herramientas que esta pone a disposición ha sido una constante en el análisis realizado.

Se podría afirmar que los resultados obtenidos en el presente trabajo de investigación son satisfactorios y que se han alcanzado los objetivos establecidos en un principio. A través de este proyecto se demuestra que el traductor especializado no puede realizar una traducción de calidad sin conocer la terminología del ámbito de especialidad al que pertenece el texto que va a traducir. Por otra parte, también evidencia la importancia que tiene conocer las estructuras formales del texto origen para poder trasladarlas adecuadamente al texto meta, ya que en algunas ocasiones hay claras diferencias culturales. Hemos abordado las dificultades que entrañan el trabajo terminológico y la traducción de un texto con un alto grado de especialización, y hemos sido capaces de detectar nuestras propias limitaciones y buscar las soluciones más adecuadas, que garantizaran unos resultados de calidad. En definitiva, hemos reflexionado y analizado los problemas reales a los que se enfrenta en su día a día un traductor profesional.

9. CONCLUSIONES

A lo largo de este trabajo de análisis e investigación se han ido desglosando todos los elementos que determinan la descripción de las características textuales, el estudio terminológico y la traducción de un texto especializado en la seguridad informática, que se considera una rama de la informática. En todo momento se ha pretendido partir de las cuestiones generales a las específicas de este tipo de proyectos con el fin de facilitar la lectura y la comprensión por parte del lector.

El desarrollo de este trabajo ha revelado las siguientes conclusiones:

En primer lugar, la necesidad de traducir este tipo de documentos es cada vez mayor debido a que desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos se han incrementado de un modo alarmante. Esto, unido a la progresiva dependencia por parte de un gran número de organizaciones de sus sistemas de información, ha provocado una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad. Es por ello que existe una necesidad real de traducciones al castellano de artículos de investigación relacionados con este campo.

En segundo lugar, el número de glosarios, diccionarios especializados y bases de datos en lengua española relacionados con este tema es muy reducido en comparación al número de recursos disponibles en inglés. Teniendo en cuenta que la seguridad informática es una ciencia en continuo proceso de construcción y expansión, existe una clara necesidad de elaborar y publicar trabajos terminológicos de este tipo. De ahí surge la idea de ampliar considerablemente las fichas del análisis terminológico de este proyecto y, por este mismo motivo, uno de los objetivos de este trabajo es su publicación. De este modo, el fichero terminológico y el glosario elaborados servirán de apoyo no solo a los profesionales de la informática que quieran estar al día de las últimas innovaciones en el ámbito de la seguridad informática, sino al conjunto de traductores, intérpretes o documentalistas neófitos en este campo.

La elaboración de glosarios específicos de cada texto, proyecto de traducción o de temas especializados facilitará la labor al traductor a la hora de realizar traducciones futuras en las que puedan aparecer en contextos similares términos ya traducidos con anterioridad. Un buen glosario o base de datos resultará una herramienta imprescindible para el traductor y el especialista. Además, como explicábamos con más detalle en apartados anteriores, las fichas terminológicas son una gran herramienta para documentalistas y traductores. Una buena base de datos con todas las fichas terminológicas recogidas sobre un tema en concreto, como es nuestro caso sobre seguridad informática, o que abarque un tema más amplio, es una gran fuente de alimentación traductológica y documentalista que facilita el trabajo en futuras traducciones o futuras documentaciones, y además enriquece al profesional en la materia en la que se esté trabajando. Lamentablemente, las ajustadas fechas de entrega rara vez lo permiten.

En definitiva, concluimos que se trata de un trabajo innovador y su publicación podría significar un paso adelante en la normalización de la terminología relacionada con la seguridad informática. Aquí encontramos un importante campo para futuras líneas de trabajo e investigación. El fin es ampliar y profundizar en la base de datos sobre seguridad informática y ponerla a disposición de traductores y estudiantes para homogeneizar la terminología en este sector.

En general, el traductor profesional, presionado por los plazos de entrega y la multitud de tareas que debe realizar en un proyecto de esta envergadura (instalación de todo el software que aparece en el manual para realizar capturas de pantalla, homogenizar el formato para adaptarse a las especificaciones, traducir, etc.), no dispone del tiempo necesario para producir terminología y sacar el máximo partido de las herramientas que esta nos brinda. Por consiguiente, se limita a usar la que ya está disponible, que, en la mayoría de los casos, no llega a satisfacer al cien por cien todas sus necesidades.

Creemos que, para cualquier persona que quiera basar su futuro profesional en el campo de la traducción especializada, la realización previa de este tipo de prácticas, fomentadas por las universidades, es absolutamente esencial para aprender lo importante que es la terminología en el proceso de la traducción. En este caso, el trabajo se ha llevado a cabo tras cinco años de práctica profesional y, sin lugar a dudas, ha propiciado una interesante reflexión

sobre la importancia de la Terminología y los problemas de tiempo a los que se enfrenta el traductor especializado.

Si conseguimos que este trabajo, al igual que otros similares, se publiquen, fomentaremos entre todos la construcción de nuevas fuentes documentales que, con el tiempo, podrían ampliarse y convertirse en herramientas que facilitarán la normalización de terminología especializada.

10. BIBLIOGRAFÍA

10.1 Libros, capítulos de libro y artículos

ACEITUNO, V.: *Seguridad de la Información, Expectativas, riesgos*. Madrid: Creaciones Copyright, 2004.

AGUILERA, P.: *Seguridad informática*. Madrid: Editex, 2010, pp. 11.

ALCARAZ VARÓ, E.: *El inglés profesional y académico.* Madrid: Alianza Editorial, 2000.

ANDERSON, M., SÁENZ-LUDLOW, A., ZELLWEGER, S. Y CIFARELLI, V. (eds.): *Educational Perspectives on Mathematics as Semiosis: From Thinking to Interpreting to Knowing*. Ottawa: LEGAS, 2003.

AREITO, J.: *Seguridad de la información redes, informática y sistemas de información*. Madrid: Paraninfo, 2008, pp. 3.

ASOCIACIÓN DE INVESTIGADORES DEL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS (CSIC): *Jornadas Internacionales de Investigación Humanística*. Madrid, 1977.

ASTON, G.: "Corpus use and learning to translate". *Textus,* 12, 1999, pp. 1000-1025.

ATKINS, S., CLEAR, J., OSTLER, N.: Corpus design criteria. *Literary and linguistic computing*, 1992, vol. 7, no 1, pp. 1-16.

BERROU, J. P.: *Para escribir bien en la empresa. Cómo redactar para ser leído y convencer*. Barcelona: Deusto, 2004.

BAZERMAN, C.: *Shaping Written Knowledge: The Genre and Activity of the Experimental Article in Science*. Madison, WI: University of Wisconsin Press, 1988.

BEEKMAN, J. Y CALLOW, J.: *Translating the word of God.* Grand Rapids: MI: Zondervan, 1974.

BELDA MEDINA, J. R.: *El lenguaje de la informática e Internet y su traducción*. Alicante: Universidad de Alicante, 2003.

BUENO, M. R.: *Lenguas para fines específicos en España a través de sus publicaciones* (1985–2002). Madrid: Córydon, 2003.

BYRNE, J.: *Technical Translation: Usability Strategies for Translating Technical Documentation*. Dordrecht: Springer, 2006.

CABRÉ, M. T.: *La terminología. Teoría, metodología, aplicaciones*. Barcelona: Editorial Antártida/Empúries, 1993.

CABRÉ, M. T.: *Actas de la 1ª reunión de profesores de terminología de las universidades españolas.* Barcelona: Universidad Pompeu Fabra, 1997.

CABRÉ, M. T.: *Actas de la 3ª reunión de profesores de terminología de las universidades españolas. Barcelona: Universidad Pompeu Fabra*, 1999.

CABRÉ, M. T.: *La terminología: Representación y comunicación*. Barcelona: IULA, 1999.

CABRÉ, M.T.: "El traductor y la terminología: necesidad y compromiso". *Panace@*, vol. 1, núm. 2, 2000, pp. 2-4.

CASAMIGLIA, H.: *Manual de análisis del discurso*. Barcelona: Ariel, 2007.

CASSANY, D.: *La cocina de la escritura*. Barcelona: Anagrama, 1995.

CHALMERS, A. F.: *¿Qué es esa cosa llamada Ciencia?* Madrid: Ed. Siglo XXI. (trad. de Eulalia Pérez Sedeño y Pilar López Máñez), 1986.

CHATFIELD C. Y JOHNSON, T.: Project 2010 (Paso A Paso). Madrid: Anaya Multimedia, 2011.

CHOMSKY, N.: *Syntactic Structures.* La Haya*:* Mouton, 1957.

CHOMSKY, N.: *Aspects of a Theory of Syntax*. Cambridge. Mass: MIT Press, 1965.

CHOMSKY, N.: *Knowledge of Language*. Nueva York: Praeger, 1986.

CHOMSKY, N.: "On the Nature, Use and Acquisition of Language". En M. Pütz (ed.) *Thirty Years of Linguistic Evolution*. Amsterdam: John Benjamins: 1992, pp. 3-29.

CONDAMINES, A.: "Un exemple d'utilisation de connaissances de sémantique lexicale", *Cahiers de Lexicologie*, 1, 1993, pp. 25-65.

CORDÓN GARCÍA, J. A., ALONSO ARÉVALO, R., GÓMEZ DÍAZ, J. Y LOPEZ LUCAS, J.*: Las nuevas fuentes de Información: información y búsqueda documental en la Web 2.0*. 2º Edición, corregida y aumentada. Madrid, Pirámide, 2012. 978-84-368-2657-9, 2010.

CORDÓN GARCÍA, J. A.: *Bibliografías nacionales y Depósito Legal: un problema documental.* Salamanca: Ediciones Universidad de Salamanca, 2002.

CROSBY, A. W.: *The Measure of Reality: Quantification and Western Society*, 1250-1600. Cambridge, MA: Cambridge University Press, 1997.

DINTEL, F.: *Cómo escribir textos técnicos o profesionales*. Barcelona: Alba Editorial 2005.

DUBUC, R. Y LAURISTON, A.: "Terms and Contexts". En *Basic Aspects of Terminology Management.* Amsterdam: John Benjamins Publishing Company, 1997.

DULANEY, E.: *CompTIA Security+ Study Guide Authorized Courseware: Exam SY0-301*, 5th Edition. Hoboken, NJ: Wiley Publishing, Inc. EE.UU., 2011.

DULANEY, E.: *Seguridad Informática. CompTIA Security+ (Títulos Especiales).* Madrid: Editorial Anaya Multimedia, 2011.

ESCOFET, A. *et al*. (eds): *Español para fines específicos. Actas del III Congreso Internacional de Español para Fines Específicos*. Utrecht: Instituto Cervantes de Utrecht, 2006, pp. 35-57.

ESCOFET, A. *et al.* (eds): "La comprensión del discurso especializado escrito en ámbitos técnico-profesionales: ¿Aprendiendo a partir del texto?" *Revista Signos,* 38(58), 2005. pp. 221-267.

ERB, U. Y KELLER, H.: *Scientific and Technical Acronyms, Symbols, and Abbreviations*. EE.UU.: John Wiley & Sons, Inc. 2001.

FERNÁNDEZ, F. Y MONTERO, B.: *La premodificación I/ominal en el ámbito de la informática. Estudio contrastivo inglés-español. Studies in English Language and Linguistics.* Valencia: Universitat de València, 2003.

FRANCIS, R. L., LEON FRANKLIN, M. G., AND WHITE J. A.: *Facility layout and location: an analytical approach.* Londres: Pearson College Division, 1992.

FRASER, A. & SANZ PINYOL, G.: *Manual de comunicaciones escritas en la empresa*, Barcelona: Interactiva, 1998.

GALLARDO SAN SALVADOR, N.: *El orden de la descripción de las características y su importancia para la denominación y traducción de un término, casos que se presentan en términos de nutrición*. Tesis doctoral sin publicar. Granada: Universidad de Granada, 1997.

GALLARDO SAN SALVADOR, N. Y SÁNCHEZ, D. (eds.): *La Enseñanza de la Terminología: Actas del Coloquio Iberoamericano sobre Enseñanza de la Terminología: Seminario sobre programa de los cursos de Terminología en la Licenciatura de Traducción e Interpretación en España*, junio 1991. Granada: Escuela Universitaria de Traductores e Intérpretes de la Universidad de Granada. 1992.

GARCÍA ARETIO, L.: (coord.). *Unidades y Guías Didácticas. Orientaciones para su elaboración*. Madrid: IUED. UNED, 1997.

GARCÍA YEBRA, V.: *Traducción y enriquecimiento de la lengua del traductor*. Madrid: Real Academia Española, 1985.

GARDARIN, G. Y VALDURIEZ, P.: *Relational Databases and Knowledge Bases*. Reading, Mass: Addison-Wesley, 1989.

GIL IRIARTE, M.L.: *Libro de estilo de ECOEM (Guía práctica para escribir mejor).* Sevilla: Fundación ECOEM, 2006.

GIRÓN ALCONCHEN, J.L.: *Introducción a la explicación lingüística de textos. Metodología y práctica de comentarios lingüísticos.* Madrid: Editorial Edinumen, 1993.

GÓMEZ DE ENTERRÍA, J.: *La comunicación escrita en la empresa.* Madrid: Arco, 2002.

GÓMEZ TORREGO, L.: *Manual del español correcto. 2 vols*. Madrid: Arco Libros. 2004.

GRIJELMO, A.: *La punta de la lengua. Críticas de humor sobre el idioma y el Diccionario.* Madrid: Aguilar, 2004.

GUTIÉRREZ RODILLA, B.M.: *La ciencia empieza en la palabra.* Capellades: Ediciones Península, S.A., 1998.

HALLIDAY, M. A. K. y HASAN, R.: *Language, Context and Text: Aspects of language in a social semiotic perspective*. Oxford: Oxford University Press, 1985.

HARTMANN, J.: *Contrastive Textology*. Heidelberg: Groos, 1987.

HUISMAN D.: iPad 2 a fondo. Madrid: Anaya Multimedia, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. ISO/R 1087-1969 *Vocabulary of Terminology*.

JONES, P. W.: *Writing Scientific Papers and Reports (5th ed.)*. Dubuque, IA: William C. Brown Publishers, 1965..

LEE-JAHNKE, H.: "Training in Medical Translation with Emphasis on German". En H. Fischbach (ed.): *Translation and Medicine*. Ámsterdam: John Benjamins, 1998, pp. 81-91.

LEE-JAHNKE, H.: "Teaching medical translation: an easy job?". *Panace@*, 6 (20), 2005, pp. 81-84.

Mcenery, T., Xiao, R., Tono, Y.: Corpus-based language studies: An advanced resource book. Ciudad: Taylor & Francis, 2006.

MAILLOT, J.: *La traduction scientifique et technique*. París: Technique et Documentation, EDISEM, 1981.

MARINKOVICH, J.: "Palabra y término: ¿Diferenciación o complementación? Discurso de incorporación a la Academia Chilena de la Lengua, como Miembro Correspondiente por Valparaíso, 20 de octubre, 2006". *Revista Signos*, 41(67), 2008, pp.119-126.

MARMEL, E. J.: *Gestión de proyectos con Project 2007*. Madrid: Anaya Multimedia, 2009.

MARTÍN VIVALDI, G.: *Curso de Redacción. Teoría y práctica de la composición y del estilo.* Madrid: Paraninfo, 2000.

MATERIAL DIDÁCTICO ESCRITO. *Módulo IV del Diplomado en Educación a Distancia.* SUA, UNAM, 2004, pp. 22-65.

MAYORAL ASENSIO, R.: "Introducción al Coloquio Iberoamericano sobre Enseñanza de la Terminología" en N. Gallardo y D. Sánchez (eds.) 1992, pp. 11-26, 1992.

MAYORAL-ASENSIO, R.: *La traducción de la variación lingüística.* Tesis doctoral sin publicar. Granada: Universidad de Granada, 1997.

MEDINA GÓMEZ, A., RUÍZ CARRASCOSA, J., HERRERA FERNÁNDEZ, J.: "Elementos que facilitan los procesos de comprensión y aprendizaje de textos". En L. García Aretio (ed.): *El material impreso en la enseñanza a distancia. Actas y congresos.* Madrid: UNED, 1997.

MELBY, A. K.: "Data Exchange Standards from the Oscar and MARTIF Projects". *Proceedings of the First International Conference on Language Resources & Evaluation* (1st LREC). Granada, 1998, pp. 3-7.

MELBY, A. K., SCHMITZ, K. D. Y WRIGHT, S. E.: "The Machine Readable Terminology Interchange Format (MARTIF): Putting Complexity in Perspective". *TermNet News* 54/55 (1996), 1997.

MONTERDE REY, A.M.: *Curso de introducción a la terminología para traductores e intérpretes*. Las Palmas de G.C.: Servicio de Publicaciones de la Universidad de Las Palmas de G.C., 1998.

MONTERO, B.: "Lengua y tecnología: aspectos terminológicos". *Terminologie et Traduction.* Valencia: Office des publications officielles des Communautés européennes. 1999, pp. 156-167.

MONTERO, B. *et al.:* "Análisis de anomalías lingüísticas: cambios producidos por la influencia del inglés en el español oral"*. Jornadas Internacionales de Lingüística Aplicada*. Granada, 1993, pp.11-15.

MONTOLÍO, E. (coord.): *Manual práctico de escritura académica*. 3 vols. Barcelona: Ariel, 2000.

NIDA, E. A.: "Linguistics and ethnology in Translation problems". *Word*, 2, 1945, pp. 194-208.

NIDA, E. A. Y TABER, C. R.: *The Theory and Practice of Translation*. Leiden: E. J. Brill, 1969.

OROSCO, M. (et al): *Informática 1.* México: Thompson, 2006.

PALOMARES PERRAUT, R.: "Evaluación de recursos documentales para el traductor en Internet." En: Pinto, M. y Cordón, J. A. (Eds.). Técnicas documentales aplicadas a la traducción. Madrid: Síntesis, 1999, pp. 179-193.

PALOMARES PERRAUT, R.: "Análisis de fuentes de información de estudios de traducción: creación de una base de datos." Málaga: Universidad, 1998.

PALOMARES PERRAUT, R.: *Recursos documentales para el estudio de la traducción.* Málaga: Universidad, 2000.

PALOMARES PERRAUT, R. Y GÓMEZ CAMARERO, C.: *Fuentes de información de publicidad y comunicación audiovisual.* Málaga: Universidad, 2002.

PAVEL, S. Y NOLET, D.: *Handbook of Terminology.* Ottawa: Public Works and Government Services Canada, 2001.

PAZ, O: *Traducción: Literatura y Literalidad.* Tusquets, Barcelona, 1990.

PÉREZ BERENGUEL, J. F.: "Glosario de errores comunes en la traducción económica y financiera". En Muñoz Martín, R. (Ed.) *I AIETI. Actas del I Congreso Internacional de la Asociación Ibérica de Estudios de Traducción e Interpretación*. Granada 12-14 de Febrero de 2003. AIETI. 619-628.

PÉREZ PRIEGO, M. A.: *La edición de textos.* Teoría de la Literatura y la Literatura comparada. Madrid: Editorial Síntesis, 1999.

PÉREZ PRIEGO, M. A.: *La edición de textos.* Segunda edición. Teoría de la Literatura y la Literatura comparada. Madrid: Editorial Síntesis, S.A. 2011.

PÉREZ PRIEGO, M. A.: "Técnicas de composición y presentación del material escrito.", en L. García Aretio, (ed.): *El material impreso en la enseñanza a distancia. Actas y congresos*. Madrid: UNED. 1997.

PICHT, H.: "Terms and their LSP environment-LSP Phraseology". *Meta,* vol. 32, nº2. 149-155, 1987.

PICHT, H.: "LSP phraseology form the terminological point of view". *Terminology Science and Research: Journal of the International Institute for Terminology Research* (IITF), 1990, vol. 1 (1990), nº 1-2- 33-48.

PICHT, H.: "Fraseología LSP (1) desde el punto de vista terminológico". *Sendebar. Boletín de la Escuela Universitaria de Traductores e Intérpretes de Granada.* Granada: Servicio de publicaciones de la Universidad de Granada, 1991.

PICHT, H.: "Lexicography-LSP Lexicography-terminography". En *IITF Journal*, vol. 6, nº 1. Viena: International network for terminology (Termnet), 1995.

PINCHUK, I.: *Scientific and Technical Translation*. André Deutsch, Londres, 1977.

POLYA, G.: *¿Cómo plantear y resolver problema?* México: Trillas, 1945.

POZO, J. I. (et al): *La solución de problemas.* Madrid: Santillana, 1994.

RAMIÓ AGUIRRE, J.: *Libro electrónico de seguridad informática y criptografía*. Material docente de libre distribución en Internet. Versión 4.1, 2006.

REYES, G.: *Cómo escribir bien en español*. Madrid: Arco Libros, 6ª ed., 2008.

RODRÍGUEZ-VIDA, S.: *Curso práctico de corrección de estilo*. Barcelona: Octaedro, 1999.

RONDEAU, G.: *Introduction a la terminologie.* Chicoutimi (Quebec): Gaëtan Morin, 1983.

ROYER, J. M.: Seguridad en la informática de empresa. Barcelona, Ediciones ENI, 2004.

SAGER, J. C.: *A practical course in terminology processing.* Amsterdam/Philadelphia: John Benjamin Publishing Company, 1990.

SAGER, J. C.: *Curso práctico sobre el procesamiento de la terminología*. Madrid: Pirámide, 1992.

SAGER, J.C.: "Future Developments and Research in Phraseology and Terminology related to Translation". *Terminologie et Traduction.* Bruselas: Servicio de Traducción de las Comunidades Europeas, vol. 2-3. Pp 584-585. 1992.

SAGER, J.C.: *Language Engineering and Translation: Consequences of automation.* Amsterdam: John Benjamins Publishing Company, 1993.

SAGER, J.C.: "Terminología para traductores, un enfoque distinto y nuevo". En *IV Congreso Internacional sobre Traducción*. Barcelona, Universidad autónoma de Barcelona, 1998.

SÁNCHEZ GIJÓN, P.: *Actas de la 2ª reunión de profesores de terminología de las universidades españolas.* Madrid: CINDOC, 1998.

SAUSSURE, F. D.: *Cours de Linguistique générale.* París: Payot, 1916.

SEQUERA, R. (ed.): *Ciencia, tecnología y lengua española: la terminología científica en español*. Madrid: Fundación Española para la Ciencia y la Tecnología, 2004.

SEPÚLVEDA, F.: "Aproximación procesual a la escritura expositiva", En L. García Aretio (ed.): *El material impreso en la enseñanza a distancia. Actas y congresos*. Madrid: UNED, 1997.

SERAFINI, M. T.: *Cómo se escribe*. Barcelona: Paidós, 1994.

SINCLAIR, J.: *Corpus, concordance, collocation.* Oxford, Nueva York: Oxford University Press, 1991a.

SINCLAIR, J.: *Council of Europe Multilingual Lexicography Project.* Informe no publicado presentado al Consejo de Europa, bajo en contrato nº 57/89, 1991b.

SINCLAIR, J.: "The automatic analysis of corpora". En J.Svartvik (ed.) *Directrions in Corpus Linguistics: Proceedings of Nobel Symposium 1982.* Berlín y Nueva York: De Gruyter, 1992, 379-397.

SINCLAIR, J.: "Corpus typology. A framework for Classification". *Comunicación en EAGLES.* Birmingham, 1994.

SINCLAIR, J.: "An international project in multilingual lexicography". En *Corpus to corpus: a study of translation equivalence. International Journal of Lexicography,* vol. 9, nº3. 1996, 9(3), 179-196.

SCHMITZ, K.D.: *Terminology Management for Translation.* Translation Technology Summer School. KU Leuven, Agosto-Septiembre, 2016.

VALDURIEZ, P.; GARDARIN, G.: Join and semijoin algorithms for a multiprocessor database machine. *ACM Transactions on Database Systems (TODS)*, 1984, vol. 9, no 1, p. 133-161.

WILBER, K.: *Eye to Eye*: *The Quest for the New Paradigm*. Boston: Shambhala, 1990.

WILLIAMS, J. M.: *Style: Ten Lessons in Clarity and Grace* (3rd ed.). Boston: Scott, Foresman and Company, 1989.

WRIGHT, S. E.: "Terminology Standarization: Management Strategies". En S. E. Wright & G. Budin (eds.) Terminology Management, 1997, pp.197-208.

WRIGHT, S. E. Y BUDIN, G.: "Data Elements in Terminological Entries: An Empirical Approach". *Terminology*. Vol. 1 nº 1. Amsterdam: John Benjamins Publishing Company, 1994.

WRIGHT, S. E. Y WRIGHT, L.: "Descriptive Terminology: Terminology Management for Technical Translation." en Wright, S. E. & G. Budin (eds.) *Handbook of Terminology Management*, Amsterdam/Philadelphia: John Benjamins, 1997, pp. 147-159.

WRIGHT, S. E. Y BUDIN, G.: *Handbook of Terminology Management* (Vol. I). Amsterdam/Philadelphia: John Benjamins, 1997.

WRIGHT, S. E. Y BUDIN, G.: *Handbook of Terminology Management* (Vol. II). Amsterdam/Philadelphia: John Benjamins. 2001.

WÜSTER, E.: *The Machine tool. An Interlingual Dictionary of basic concepts.* Londres: Pergamon, 1968.

ZANETTIN, F.: "DIY Corpora: The WWW and the Translator". En B. Maia, J. Haller y M. Urlrych (eds.). *Training the Language Services Provider for the New Millennium.* Oporto: Facultade de Letras, Universidade do Porto, 2002, pp. 239-248.

10.2 Diccionarios

AGUADO DE GEA, G.: *Diccionario comentado de términos informáticos*. Madrid: Paraninfo, 1994.

AHUMADA, I. (ed.): *Diccionario bibliográfico de la metalexicografía del español.* Jaén: Universidad, 2006.

ALARCÓN ÁLVAREZ, E.: *Diccionario de términos informáticos e Internet*. Madrid: Anaya Multimedia, 2007.

DÍAZ DE SANTOS: *Diccionario de Informática*. Madrid: Publicado originalmente en Oxford University Press [Trad. Por B. Mendizábal: Madrid], 1993.

DICTIONARY OF COMPUTING [2ª ed.]: Nueva York: Oxford University Press, 1986.

ENCYCLOPAEDIA BRITANNICA. [Fecha de consulta: 25 de octubre, 2013] <http://www.britannica.com/EBchecked/topic/339421/library>

MARTÍNEZ-VAL, J. M.: *Diccionario Enciclopédico de Tecnología*. Madrid: Editorial Síntesis, 2000.

MCGRAW HILL ENCYCLOPEDIA OF SCIENCE & TECHNOLOGY. Nueva York: McGraw-Hill Companies, Inc. 2007.

MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY. [Fecha de consulta: 25 de octubre, 2013] <http://www.merriam-webster.com/>

MICROSOFT CORPORATION: *Diccionario de Informática e Internet de Microsoft (2.ª edición)*. Nueva York: McGraw-Hill Companies, Inc. 2004.

MICROSOFT TERMINOLOGY. Language Portal. Consultado el 25 de abril de 2013 <http://www.microsoft.com/Language/en-US/Default.aspx>

OXFORD ENGLISH DICTIONARY (*OED*). Oxford: Oxford University Press.

PALAU Y DULCET, A.: *Manual del librero hispanoamericano*. Barcelona: Palau, 1975.

PARKER, S.: *Diccionario McGraw-Hill de Computación* [Trad. Por J.O. Sánchez y M.C.Canales]. Madrid: MacGraw-Hill, 1986.

PARKER, S. P.: *McGraw-Hill Dictionary of Scientific and Technical Terms (sixth edition)*. McGraw-Hill Companies, Inc. 2003.

RAE: *Diccionario de la lengua castellana*. 22ª edición, 2001.

REAL ACADÉMICA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES: *Vocabulario científico y técnico*. Madrid: Editorial Espasa Calpe, S.A., 1996.

REAL ACADÉMICA DE CIENCIAS EXACTAS, FÍSICAS Y NATURALES: *Diccionario esencial de las ciencias*. Madrid: Editorial Espasa Calpe, S.A., 2002.

SALVÁ, V.: *Nuevo diccionario de la lengua castellana*. Alicante: Biblioteca Virtual Miguel de Cervantes, 2006. (Original: París: Vicente Salvá, 1846).

SMITH, C. et al.: *Collins Spanish-Eng/ish/English-Spanish Dictionary.* Barcelona: Grijalbo, 1992.

SY0-201 MATERIALES DE ESTUDIO. [Fecha de consulta: 3 de abril, 2013] <http://es.prmob.net/comptia/tecnolog%C3%ADa-de-la-informaci%C3%B3n/microsoft-certified-professional-1636828.html>

UNE 1-070. *Vocabulario de la terminología*. Madrid: IRANOR, 1979.

10.3 Páginas Web

ASOCIACIÓN ESPAÑOLA DE TERMINOLOGÍA. [Fecha de consulta: 20 de diciembre, 2016] <http://www.aeter.org/?page_id=75>

APARICI, R.: *El documento integrado*. [Fecha de consulta: 14 de agosto, 2013] <http://usuarios.lycos.es/saraoa/integra.html>

CABRÉ, M. T.: "La Terminología hoy: concepciones, tendencias y aplicaciones", *Ciência de Informação,* Vol. 24, nº 3, 1995. [Fecha de consulta: 15 de enero, 2013] <http://www.ibict.br/cienciadainformacao/include/getdoc.php?id=876&article=530&mode=pdf>.

CABRÉ, M. T.: "La Teoría Comunicativa de la Terminología, una aproximación lingüística a los términos", Revue française de linguistique appliquée, 2/2009 (Vol. XIV), p. 9-15. 2009. [Fecha de consulta: 20 de diciembre, 2016] <http://www.cairn.info/revue-francaise-de-linguistique-appliquee-2009-2-page-9.htm>

CHANTAL PÉREZ HERNÁNDEZ, M.: "Explotación de los córpora textuales informatizados para la creación de bases de datos terminológicas basadas en el conocimiento. Estudios de Lingüística del Español (ELiEs)." Universidad de Málaga 2002. [Fecha de consulta: 30 de agosto, 2015]. <http://elies.rediris.es/elies18/index.html>

CISCO NETWORKING ACADEMY. [Fecha de consulta: 8 de septiembre, 2014] <http://cisco.infomerce.es/CCNA_RS/course/module11/11.2.3.2/11.2.3.2.html>

DEDOLME, S.: *Aspectos didácticos a tener en cuenta en la estructuración de materiales impresos*. UNED. [Fecha de consulta: 14 de agosto, 2013] <http://seduca.uaemex.mx/prog_dist/curso/edu_dist/uploads/discpedagmded.pdf>

GAMERO, S.: *Introducción a la traducción técnica*. Jaén, 2005. [Fecha de consulta: 8 de septiembre, 2014] <http://www3.uji.es/~gamero/traductortecnico.pdf>

GUTIÉRREZ ASCENCIO, F.: *Texto didáctico.* Diseño de cursos en línea. Selección de materiales didácticos. Universidad Autónoma del Estado de Hidalgo. Sistema de universidad virtual. 2009. [Fecha de consulta: 8 de septiembre, 2014] <http://cvonline.uaeh.edu.mx/Cursos/ObjetosAprendizaje/Novena/mod2/v1/seleccion/lec_texto_didactico.pdf>

IBM Knowledge Center: Tipos de cifrado y modalidades de cifrado. [Fecha de consulta: 8 de septiembre, 2014] <http://www.ibm.com/support/knowledgecenter/es/SSGU8G_12.1.0/com.ibm.sec.doc/ids_en_010.htm>

IULA: "La terminología: definición y funciones", en Grup IulaTerm, 2004a. [Fecha de consulta: 3 de noviembre, 2013] <http://www.iulaonline.org>

IULA: "La terminología: historia y organización", en Grup IulaTerm, 2004b. [Fecha de consulta: 3 de noviembre, 2013] <http://www.iulaonline.org>

IULA: "Terminología y enseñanza de lenguas", en Grup IulaTerm, 2004c. [Fecha de consulta: 3 de noviembre, 2013] <http://www.iulaonline.org>

IULA: "Terminología y traducción", en Grup IulaTerm, 2004d. [Fecha de consulta: 3 de noviembre, 2013] <http://www.iulaonline.org>

IULA: "La unidad de trabajo del discurso especializado", en Grup IulaTerm.2004e. [Fecha de consulta: 3 de noviembre, 2013] <http://www.iulaonline.org>

IULA: "Terminología: Origen, Definición y Aplicación", en Grup IulaTerm, 2005. [Fecha de consulta: 3 de noviembre, 2013] <http://www.iulaonline.org>

MONTERO FLETA, B.: "Terminología científica: Préstamos, Calcos y Neologismos" en *Actas XXXIX Congreso de AEPE.* Segovia: Centro Virtual Cervantes, 2004, pp. 41-57. [Fecha de consulta: 3 de noviembre, 2013] <http://cvc.cervantes.es/ensenanza/biblioteca_ele/aepe/pdf/congreso_39/congreso_39_07.pdf>

PONCE MÁRQUEZ, N.: "Diferentes aproximaciones al concepto de equivalencia en traducción y su aplicación en la práctica profesional", *Tonos Digital 15. Revista Electrónica de Estudios Filológicos.* Junio, 2008. [Fecha de consulta: 4 de noviembre, 2013]
<http://www.tonosdigital.es/ojs/index.php/tonos/article/viewFile/210/170>

RAMIÓ AGUIRRE, J.: *Libro electrónico de seguridad informática y criptografía.* Material docente de libre distribución en Internet. Versión 4.1, 2006. . [Fecha de consulta: 21 de diciembre, 2016]
<http://bioinfo.uib.es/~joemiro/aenui/procJenui/ProcWeb/actas2001/raint73.pdf>

SANTAMARÍA, F.: *Herramientas colaborativas para la enseñanza usando tecnologías WEB: Redblogs, Redes Sociales, Wikies, Web 2,* 2005. [Fecha de consulta: 14 de agosto, 2015]
<http://gabinetedeinformatica.net/descargas/herramientas_colaborativas2.pdf>

SEVILLA MÚÑOZ, M. Y MACÍAS OTÓN, E.: Terminología. Módulo I: Introducción a la terminología. OpenCourseWare. Universidad de Murcia, 2008. [Fecha de consulta: 14 de agosto, 2015]
<http://ocw.um.es/cc.-sociales/terminologia/material-de-clase-1/modulo-i.pdf>

TERCEDOR SÁNCHEZ, M.: *La fraseología en el lenguaje biomédico: análisis desde las necesidades del traductor*. Vol. 6., 1999. [Fecha de consulta: 14 de agosto, 2015]
<http://elies.rediris.es/elies6/index.html#indice>

TUTORIAL PAVEL DE TERMINOLOGÍA: Oficina de Traducciones del Gobierno de Canadá, 2008. [Fecha de consulta: 14 de agosto, 2015]
<http://termiumplus.gc.ca/didacticiel_tutorial/espanol/lecon1/page1_2_4_s.htm l>

11. ANEXOS

Anexo I: Texto meta

Capítulo 5. Infraestructura y conectividad

<Cuerpo texto>En este capítulo se tratan los siguientes objetivos del examen CompTIA Security+:
<Sep-med>1.1 Explicar la función y el propósito de seguridad de los dispositivos y tecnologías de red.
1.3 Distinguir y diferenciar elementos y compuestos de red.
1.4 Implementar y utilizar protocolos comunes.
1.5 Identificar puertos de red predeterminados utilizados con frecuencia.
2.8 Ejemplificar los conceptos de confidencialidad, integridad y disponibilidad.
4.2 Llevar a cabo los procedimientos adecuados para establecer la seguridad host.
<Cuerpo texto>Este capítulo le presenta el hardware que utiliza en la red. Este se compone de una serie de medios y dispositivos que facilitan las comunicaciones y proporcionan seguridad. La mayoría de dichos dispositivos (enrutadores, módems y sistemas PBX) proporcionan conectividad externa desde su red a otros sistemas y redes. Para ofrecer una protección razonable, debe saber cómo funcionan los mencionados dispositivos y de qué forma proporcionan o no seguridad.
El presente capítulo trata cuestiones de infraestructura, puertos de red y protocolos comunes. Son elementos clave para el examen Security+ y, además, es necesario entenderlos para asegurar su red. Sin embargo, al igual que muchos otros exámenes de certificación, la prueba Security+ no solo requiere que conozca las tecnologías actuales, sino también algunos componentes de legado.
<Nivel 1>Descubrir TCP/IP
<Cuerpo texto>TCP/IP ha sido una salvación para las organizaciones que necesitan conectar de forma conjunta varios sistemas con el fin de que funcionen como un todo unificado. Por desgracia, una de las desventajas que incorpora una red fácil de usar y utilizada durante años es que presenta numerosos agujeros. Puede cerrar la mayoría de ellos con facilidad, pero primero debe saber en qué consisten.
<Nota>**Nota:** Necesitará conocer en profundidad los procesos que utiliza TCP/IP para saber cómo funcionan los ataques sobre este. El énfasis de esta sección recae sobre los tipos de conexiones y servicios. Si no conoce bien estas áreas, es recomendable que complemente su estudio con información básica acerca de redes que puede encontrar en la Web.
<Cuerpo texto>Las siguientes secciones se centran en cuestiones relacionadas con TCP/IP y seguridad. Muchas de ellas le resultarán familiares si se ha presentado a los exámenes Network+ o Server+ de CompTIA. No obstante, si tiene alguna laguna sobre el tema, no dude en leer cuidadosamente las siguientes secciones.
<Nota>**Nota:** Cuando se habla de redes, se suele hacer referencia al modelo de siete capas OSI, considerado durante mucho tiempo como el patrón de funcionamiento de los protocolos de red. TCP/IP precede a la creación del modelo OSI y, por esta razón, lleva a cabo las mismas funciones, aunque con cuatro capas en lugar de siete.
<Nivel 2>Trabajar con el entorno TCP/IP
<Cuerpo texto>El entorno TCP/IP se divide en cuatro capas arquitectónicas:
<Sep-med>* Capa Aplicación.
* Capa Host-a-host o Transporte.
* Capa Internet.
* Capa Acceso de red (también conocida como la capa Interfaz de red o Enlace).
<Cuerpo texto>Los ordenadores que utilizan TCP/IP emplean la conexión física existente entre los sistemas. TCP/IP no se refiere a la topología de red, ni a las conexiones físicas. El controlador de red que reside en un ordenador o host gestiona el protocolo físico o la topología. TCP/IP se comunica con este controlador y le permite interesarse por la topología de red y la conexión física.
En términos de TCP/IP, un ordenador en la red es un host. A su vez, un host es cualquier dispositivo conectado a la red que ejecute un entorno o pila de protocolo TCP/IP. La figura 2.1 muestra las cuatro capas de una pila de protocolo TCP/IP. Tenga en cuenta que esta ilustración incluye la topología física o de red. Aunque no forma parte de TCP/IP, la topología es esencial para conducir información en una red.
**********2_001.tif**********
<Pie figura>**Figura 2.1.** Las capas de la arquitectura TCP/IP.
<Cuerpo texto>Las cuatro capas de TCP/IP cuentan con funciones y métodos únicos para llevar a cabo su trabajo. Cada capa se comunica con las que residen arriba y abajo. Además, cada una de ellas tiene sus propias reglas y capacidades.
Las siguientes secciones describen las capas específicas de TCP/IP, así como los protocolos comunes que se utilizan en la pila y el modo en que se transmite la información entre ellas. También se explican algunos de los métodos más frecuentes para atacar a las redes TCP/IP.
La encapsulación, es decir, el proceso que se utiliza para transmitir mensajes entre las capas en TCP/IP, se trata con brevedad una vez que se hayan explicado las capas.

<Nivel 3>La capa Aplicación
<Cuerpo texto>Aplicación es la capa superior del entorno. Permite a las aplicaciones acceder a servicios o protocolos para intercambiar datos. La mayoría de los programas, por ejemplo, los navegadores Web, interactúan con TCP/IP en este nivel. Los protocolos más utilizados en la capa Aplicación son los siguientes:
<Sep-med>* **HTTP (*Hypertext Transfer Protocol*, Protocolo de transferencia de hipertexto):** Este es el protocolo que se utiliza para las páginas Web y World Wide Web. Las aplicaciones de HTTPutilizan un lenguaje estándar llamado HTML (*Hypertext Markup Language*, Lenguaje de marcado de hipertexto). Los archivos HTML son archivos normales de texto que contienen un código especial que permite que un navegador Web u otras aplicaciones Web habilitadas visualicen gráficos, fuentes especiales y caracteres.
* **HTTPS (*HTTP Secure*, HTTP seguro):** Este protocolo se utiliza para páginas Web "seguras" que el usuario debe utilizar cuando introduce información personal como números de tarjetas de crédito, contraseñas y otros identificadores. Este combina HTTP con SSL/TLS con el fin de proporcionar comunicación cifrada. El puerto predeterminado es 443 y la URL comenzará por https:// en lugar de http://. En un principio, Netscape creó este protocolo para utilizarlo con su navegador y acabó convirtiéndose en un estándar con RFC 2818 (que puede encontrar en http://www.ietf.org/rfc/rfc2818.txt).
* **FTP (*File Transfer Protocol*, Protocolo de transferencia de ficheros):** Esta es una aplicación que permite conectarse a los servidores FTP para subir y descargar archivos. Se trata de una aplicación frecuente para transferir archivos entre host pero resultainsegura. Ya se han publicado algunas opciones para crear un protocolo que esté libre de todo peligro, entre ellas se incluyen FTPS (*FTP over SSL*, FTP sobre SSL), que añade soporte a la criptografía SSL, y SFTP (SSH, *File Transfer Protocol*, Protocolo de transferencia de ficheros), también conocido como FTP seguro.
Una utilidad alternativa para copiar archivos es SCP (*Secure Copy*, Copia segura) que combina un antiguo RCP (*Remote Copy Program*, Programa de copia remota) desde los inicios de TCP/IP con SSH. En el extremo opuesto, desde el punto de vista de seguridad, está TFTP (*Trivial File Transfer Protocol*, Protocolo trivial de transferencia de archivos), que puede configurarse para transferir archivos entre host sin ninguna interacción con el usuario (modo desentendido) y que debería evitar a toda costa.
* **SMTP (*Simple Mail Transfer Protocol*, Protocolo simple de transferencia de correo):** Protocolo estándar para comunicaciones de correo electrónico. SMTP permite a los clientes y servidores de correo comunicarse mediante el envío de mensajes.
* **Telnet:** Terminal interactiva que simula un protocolo. Permite a un usuario remoto iniciar una sesión interactiva con un servidor Telnet. Al cliente puede parecerle que se trata de una sesión local.
* **DNS (*Domain Name System*, Sistemas de nombres de dominio):** Permite al host resolver nombres de una dirección IP (*Internet Protocol*, Protocolo de Internet).
* **RIP (*Routing Information Protocol*, Protocolo de información de enrutamiento):** Permite que la información de enrutamiento se intercambie entre los enrutadores en una red IP.
* **SNMP (*Simple Network Management Protocol*, Protocolo simple de administración de redes):** Se trata de una herramienta de gestión que permite la comunicación entre dispositivos de red y una consola de administración. La mayoría de enrutadores, puentes y concentradores inteligentes pueden comunicarse usando SNMP.
* **POP (*Post Office Protocol*, Protocolo de oficina de correos):** Protocolo utilizado en muchos sistemas de correo electrónico. Este permite características avanzadas y es una interfaz estándar en muchos servidores de correo electrónico. POP se emplea para recibir correo.
<Nota>**Nota:** Uno de los aspectos clave que debe conocer cuando asegure una red es que solo esté utilizando los protocolos necesarios para las operaciones. Compruebe que se han eliminado todos los protocolos anticuados, los que ya no necesita. Si no los elimina, estará dejando una puerta abierta a un atacante que quiera acceder a su sistema a través de las debilidades del protocolo en cuestión.
<Nivel 3>Capa Transporte o Host-a-host
<Cuerpo texto>La capa Host-a-host, también conocida como capa Transporte, proporciona a la capa Aplicación una sesión y servicios de comunicación de datagramas. Los protocolos TCP (*Transmission Control Protocol*, Protocolo de control de transmisión) y UDP (*User Datagram Protocol*, Protocolo de datagramas de usuario) operan en esta capa. Ambos proporcionan gran parte de la funcionalidad de la red TCP/IP.
El protocolo TCP es el responsable de proporcionar una sesión fiable, uno a uno, orientada a la conexión. TCP establece una conexión y asegura que el otro extremo recibe los paquetes. Dos host se comunican el resultado de los paquetes entre sí. TPP también asegura que los paquetes se descodifican y se secuencian correctamente. Esta conexión persiste durante la sesión y desaparece al finalizar esta..
El UDP proporciona un método de comunicación sin conexión no fiable entre dos host. Se trata de un protocolo de servicio mínimo, pero bastante más rápido que TCP. Las sesiones no establecen una sesión sincronizada como la que utiliza TCP y no garantiza que las comunicaciones estén libres de errores. El propósito principal de UDP es enviar pequeños paquetes de información. La aplicación es la responsable de interpretar la recepción correcta de datos.
<Nivel 3>La capa Internet
<Cuerpo texto>La capa Internet es responsable del enrutamiento, el direccionamiento IP y el empaquetado. Los protocolos de la capa Internet realizan la mayoría de las tareas internas que otorgan la habilidad de intercambiar información entre host. A continuación, encontrará los cuatro protocolos estándar de la capa Internet:
<Sep-med>* **IP (*Internet Protocol*, Protocolo de Internet):** Protocolo enrutable responsable del direccionamiento IP. Además, fragmenta y vuelve a ensamblar los paquetes del mensaje. Redirige la información pero no verifica su precisión, ya que esto es tarea de TCP. IP determina si un destino es conocido y, si lo es, redirige la información hacia allí. Si el destino es desconocido, envía el paquete al enrutador, que lo envía.

* **ARP (*Address Resolution Protocol*, Protocolo de resolución de direcciones):** Protocolo responsable de resolver las direcciones IP para la capa Interfaz de red, incluyendo las direcciones de hardware. ARP puede resolver una dirección IP para un identificador MAC (*Media Access Control*, Control de acceso a medios). Las direcciones MAC se utilizan para reconocer dispositivos de hardware de red, por ejemplo, una NIC (*Network Interface Card*, Tarjeta de interfaz de red).
<Nota>**Nota:** Observará que el acrónimo MAC se utiliza con mucha frecuencia. También se emplea para identificar *Mandatory Access Control* (Control de acceso obligatorio), que define cómo actúa el control de acceso en un modelo de autenticación. También lo encontrará en el contexto de la criptografía, en el que significa *Message Authentication Code* (Código de autentificación de mensajes), que verifica la precisión de un algoritmo.
<Sep-med>* **ICMP (*Internet Control Message Protocol*, Protocolo de mensajes de control de Internet):** Este protocolo proporciona funciones de mantenimiento e informes. Lo utiliza el programa Ping. Cuando un usuario quiere comprobar la conectividad de otro host, puede introducir el comando **PING** con la dirección IP y el sistema hará lo oportuno. Si la conectividad es buena, ICMP devolverá datos al host original. Por otro lado, ICMP le comunicará si un destino es inaccesible. Los enrutadores y otros dispositivos de red comunican la información de ruta entre dos host con ICMP.
* **IGMP (*Internet Group Management Protocol*, Protocolo de administración de grupos de Internet):** Este protocolo es el principal responsable de gestionar los grupos de multidifusión IP. Éstos pueden enviar mensajes o paquetes a un grupo específico de host. No es lo mismo que una trasmisión, que reciben todos los usuarios en una red.
<Nivel 3>La capa Acceso de red
<Cuerpo texto>El nivel más bajo del entorno TCP/IP es la capa Acceso de red (o Interfaz). Esta capa es responsable de colocar y eliminar paquetes en la red física a través de comunicaciones con los adaptadores de red en el host. Este proceso permite a TCP/IP trabajar con casi cualquier tipo de topología o tecnología de red, así como con pequeñas modificaciones. Si se instalara una nueva topología de red física, por ejemplo, una conexión de fibra Ethernet de 10 GB, TCP/IP solo necesitaría saber cómo comunicarse con el controlador de red para que su funcionamiento sea correcto. TCP/IP también puede interactuar con más de una topología de red al mismo tiempo. Esto permite que el protocolo pueda utilizarse en casi cualquier entorno.
<Nivel 2>IPv4 versus IPv6
<Cuerpo texto>El entorno del protocolo TCP/IP que se utiliza hoy en día ha estado presente desde los comienzos de Internet, antes incluso de que se conociera por ese nombre. Lo destacable de este hecho es que ha podido evolucionar al nivel de uso actual gracias al pensamiento avanzado de los que estuvieron involucrados en su creación.
Sin embargo, hace algunos años, cundió el pánico al pensar que no habría suficientes direcciones IP para asignarlas a todos los host que necesitaran conectarse. El sistema de numeración actual, conocido como IPv4 (*IP version 4*, IP versión 4) aunque en realidad no se hayan publicado versiones anteriores, es el objeto de este capítulo y todavía se utiliza hoy en día. IPv6 (*IP version 6*, IP versión 6) se presentó hace algunos años para reemplazar a IPv4 pero ha fracasado en su intento y la mayoría de sistemas suelen ser compatibles con las dos en la capa Internet.
Las ideas clave que tiene que tener en cuenta para el examen son las siguientes: IPv6 es compatible con direcciones de 128 bit, mientras que IPv4 admite direcciones de 32 bit. Asimismo, IPv6 incluye seguridad IPSec obligatoria.
<Nivel 2>La encapsulación
<Cuerpo texto>Uno de los puntos esenciales para entender este proceso en capas es el concepto de la encapsulación. Este permite que un protocolo de transporte se envíe a través de la red para que la utilice el servicio o protocolo equivalente en el host receptor. En la figura 2.2 puede observar cómo se encapsula el correo electrónico cuando se traslada desde los protocolos de la aplicación a través de los protocolos de transporte e Internet. Cada una de las capas añade información de encabezado cuando el correo electrónico cuando baje entre las capas.
**********2_002.tif**********
<Pie figura>**Figura 2.2.** Proceso de encapsulación de un mensaje de correo electrónico.
<Cuerpo texto>La transmisión del paquete entre los dos host se produce a través de la conexión física en el adaptador de red. La figura 2.3 ilustra este proceso entre dos host. Puede que el contenido de la figura no sea muy exhaustivo, pero plasma el proceso de la transmisión de mensajes.
**********2_003.tif**********
<Pie figura>**Figura 2.3.** Un cliente envía un mensaje de correo electrónico a un servidor a través de Internet.
<Cuerpo texto>Una vez que se encapsula, el mensaje se envía al servidor. Tenga en cuenta que en la figura 2.3 el mensaje se envía a través de Internet, podría ser tan sencillo como enviarlo de forma local. El cliente del correo electrónico no sabe cómo se entrega el mensaje y a la aplicación del servidor no le interesa cómo ha llegado allí. Esto hace que diseñar e implementar servicios como el correo electrónico sean posibles en un entorno global o de Internet.
<Nivel 2>Trabajar con protocolos y servicios
<Cuerpo texto>Es esencial que cuente con un entendimiento básico de los protocolos y servicios para aprobar el examen. Aunque no es un requisito, CompTIA recomienda que tenga la certificación Network+ antes de presentarse a este examen. En caso de que no esté muy familiarizado con ciertas áreas, las siguientes secciones tratan de forma detallada cómo se comunican entre sí los host TCP/IP. Además, se describen los conceptos de puertos, protocolos de enlace e interfaces de aplicación. El objetivo no es que se convierta en un experto en la materia, sino facilitarle el aprendizaje de lo que se encontrará cuando intente asegurar una red TCP/IP.
<Nota>**Nota:** La mayoría de explicaciones de este libro se centran en TCP/IP como protocolo de red, ya que se utiliza en casi todas las implementaciones. Sin embargo, debe saber que TCP/IP no es el único protocolo de red y que la implementación de Microsoft NetBIOS (*Network Basic Input Output System*, Sistema básico de entrada y salida de red) era la predeterminada en versiones anteriores de Windows. Desde entonces, NetBIOS se ha adaptado para

ejecutarse sobre TCP/IP y todavía se usa de forma generalizada para la resolución y el registro de nombres en entornos basados en Windows.
<Nivel 3>Los puertos más conocidos
<Cuerpo texto>En resumidas cuentas, los puertos identifican cómo se produce un proceso de comunicación. Éstos son direcciones especiales que posibilitan la comunicación entre host. Se añade un número de puerto desde el origen, indicando qué puerto se comunica con el servidor. Si este tiene un puerto definido y disponible para uso, enviará un mensaje de vuelta aceptando la solicitud. Si el puerto no es válido, el servidor rechazará la conexión. La IANA (*Internet Assigned Numbers Authority*, Autoridad de números asignados a Internet) ha definido una lista de puertos denominada "Puertos más conocidos".
<Nota>**Nota:** Puede encontrar la descripción completa de los puertos definidos por la IANA en el siguiente sitio Web: www.iana.org/assignments/port-numbers. Hay miles de puertos disponibles para servidores y clientes.
<Cuerpo texto>Un puerto no es otra cosa que un bit de información adicional añadido a un mensaje TCP o UDP. Esta información se incluye en el encabezado del paquete. La capa inferior encapsula el mensaje con su encabezado. Muchos de los servicios que empleará cuando esté en Internet utilizarán los números de puerto TCP que aparecen en la tabla 2.1. Por otra parte, la tabla 2.2 identifica algunos de los puertos UDP más frecuentes y conocidos. Podrá observar que algunos servicios emplean puertos TCP y UDP, mientras que otros solo recurren a uno de ellos.
<Pie figura>**Tabla 2.1.** Los puertos TCP más conocidos.
<Tablas>**Número de Puerto TCP** **Servicio**
20 FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos) (canal de datos).
21 FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos) (canal de control).
22 SSH (*Secure Shell*, Intérprete de órdenes segura) y SCP (*Secure Copy*, Copia segura).
23 Telnet (*Telecommunication Network*, Red de telecomunicaciones).
25 SMTP (*Simple Mail Transfer Protocol*, Protocolo Simple de Transferencia de Correo).
49 TACACS (*Terminal Access Controller Access Control System*, Sistema de control de acceso mediante control del acceso desde terminales) para servicio de autenticación.
80 HTTP (*Hypertext Transfer Protocol*, Protocolo de transferencia de hipertexto) (utilizado para World Wide Web).
110 POP3 (*Post Office Protocol*, Protocolo de la oficina de correo)
115 SFTP (*Secure File Transfer Protocol*, Protocolo de transferencia de archivos seguro).
119 NNTP (*Network News Transport Protocol*, Protocolo de transferencia de noticias en red).
137 NetBIOS (*Network Basic Input/Output System*, Sistema básico de entrada y salida de red) para servicio de nombre.
138 NetBIOS (*Network Basic Input/Output System*, Sistema básico de entrada y salida de red) para servicio de datagrama.
139 NetBIOS (*Network Basic Input/Output System*, Sistema básico de entrada y salida de red) para servicio de sesión).
143 IMAP (*Internet Message Access Protocol*, Protocolo de acceso a mensajes de Internet).
389 LDAP (*Lightweight Directory Access Protocol*, Protocolo Ligero de Acceso a Directorio).
443 HTTPS (*HTTP Secure*, HTTP seguro) (utilizado para conexiones Web seguras).
989 FTPS (*FTP over SSL*, FTP sobre SSL) (canal de datos).
990 FTPS (*FTP over SSL*, FTP sobre SSL) (canal de control).
<Pie figura>**Tabla 2.2.** Los puertos UDP más conocidos.
<Tablas>**Número de Puerto UDP** **Servicio**
22 SSH (*Secure Shell*, Intérprete de órdenes segura) y SCP (*Secure Copy*, Copia segura).
49 TACACS (*Terminal Access Controller Access Control System*, Sistema de control de acceso mediante control del acceso desde terminales) para servicio de autenticación.
53 DNS (*Domain Name System*, Sistema de nombres de dominio) para consultas de nombre
69 TFTP (*Trivial File Transfer Protocol*, Protocolo trivial de transferencia de archivos).
80 HTTP (*Hypertext Transfer Protocol*, Protocolo de transferencia de hipertexto) (utilizado para World Wide Web).
137 NetBIOS (*Network Basic Input/Output System*, Sistema básico de entrada y salida de red) para servicio de nombre.
138 NetBIOS (*Network Basic Input/Output System*, Sistema básico de entrada y salida de red) para servicio de datagrama.
139 NetBIOS (*Network Basic Input/Output System*, Sistema básico de entrada y salida de red) para servicio de sesión.
143 IMAP (*Internet Message Access Protocol*, Protocolo de acceso a mensajes de Internet).
161 SNMP (*Simple Network Management Protocol*, Protocolo Simple de Administración de Red).
389 LDAP (*Lightweight Directory Access Protocol*, Protocolo Ligero de Acceso a Directorio).
989 FTPS (*FTP over SSL*, FTP sobre SSL) (canal de datos).
990 FTPS (*FTP over SSL*, FTP sobre SSL) (canal de control).
<Cuerpo texto>La documentación anterior de estos puertos especifica que los puertos inferiores a 1024 están reservados para uso administrativo. No obstante, el cumplimiento de esta restricción es voluntario y ocasiona problemas a los profesionales de la seguridad informática. Como puede observar, cada uno de estos puertos requiere, en principio, distintas medidas de seguridad, dependiendo de la aplicación a la que se asignen. Todos los puertos permiten acceso a su red; incluso si configura un cortafuegos, debe mantener estos puertos abiertos si quiere proporcionar servicios de correo electrónico o Web.

En el ejercicio 2.1 aprenderá cómo ver los puertos TCP y UDP (*User Datagram Protocol*, Protocolo de datagramas de usuario) activos.
**********Inicio ejercicio**********
<Nivel 4>Ejercicio 2.1. Ver los puertos TCP y UDP activos.
<Cuerpo texto>Como administrador, debería saber qué puertos están activados en su servidor. Para ver los puertos TCP y UDP activos, siga estos pasos:
<Sep-med>1. Diríjase a **Símbolo del sistema**. En Windows, escriba **CMD** en la línea de comandos. En un servidor Linux, abra una ventana de comandos.
2. Escriba el comando **netstat** (véase la figura 2.4).
**********2_004.tif**********
<Pie figura>**Figura 2.4.** Resultados del comando netstat.
<Sep-med>3. Deberían aparecer algunos elementos. A continuación, escriba **netstat -a**. El parámetro **-a** comunica a netstat que visualice toda la información.
4. Observe todos los puertos que se enumeran (véase la figura 2.5).
**********2_005.tif**********
<Pie figura>**Figura 2.5.** Resultados del comando netstat -a.
<Sep-med>5. Vea el archivo services (systemroot\system32\drivers\etc\services en Windows o /etc/services en Linux). Aunque el sistema no puede leerlo de forma activa, este archivo enumera los servicios y los puertos utilizados con más frecuencia en las operaciones de red.
**********2_006.tif**********
<Pie figura>**Figura 2.6.** Contenido del archivo Services.
**********fin ejercicio**********
<Nivel 3>Protocolo de enlace TCP en tres direcciones
<Cuerpo texto>TCP, que está orientado a la conexión, establece una sesión usando un protocolo de enlace en tres direcciones. Un host llamado cliente origina dicha conexión yel cliente envía un segmento TCP o mensaje al servidor. Este segmento del cliente incluye un ISN (*Initial Sequence Number*, Número de secuencia inicial) para la conexión y un tamaño de ventana. A continuación, el servidor responde con un segmento TCP que contenga su ISN y un valor en el que se indica su búfer o tamaño de ventana. Finalmente, el cliente envía de vuelta una solicitud del número de secuencia del servidor.
La figura 2.7 muestra este protocolo de enlace en tres direcciones que tiene lugar entre un cliente y un servidor. Cuando concluya la sesión o conexión, se producirá un proceso similar, usando cuatro pasos para cerrar la conexión.
**********2_007.tif**********
<Pie figura>**Figura 2.7.** Proceso de conexión TCP.
<Cuerpo texto>Una solicitud Web utiliza el proceso TCP para establecer la conexión entre el cliente y el servidor. Cuando esto ocurre, los dos sistemas se comunican entre sí. Para ello, el servidor emplea el puerto TCP número 80. Ocurre lo mismo si se realiza una conexión de correo electrónico, con la diferencia de que el cliente (suponiendo que está usando POP3) usa el puerto 110.
De este modo, un servidor puede gestionar varias solicitudes de forma simultánea. Cada sesión tiene distinto número de secuencia, aunque todas utilicen el mismo puerto. Todas las comunicaciones de una sesión determinada emplean este número de secuencia para evitar que se confundan las sesiones.
<Nivel 3>Interfaz de programación de aplicaciones
<Cuerpo texto>Crear una interfaz para TCP/IP es mucho más simple que para los modelos de red anteriores. La mayoría de empresas de software ponen a su disposición un grupo bien definido y establecido de API (*Application Programming Interfaces*, Interfaces de programación de aplicaciones). Las API permiten a los programadores crear interfaces para el protocolo. Cuando un programador necesita crear una aplicación Web habilitada, pueden llamar o utilizar una de estas API con el fin de realizar la conexión, enviar o recibir datos y finalizar dicha conexión. Las API están escritas con anterioridad y hacen que el trabajo sea bastante más fácil que si se tuviera que escribir el código de forma manual con toda la información de la conexión.
Microsoft utiliza la API Windows Sockets (Winsock) para que sirva como interfaz del protocolo. Puede acceder a los protocolos TCP o UDP para realizar las tareas que necesite. La figura 2.8 ilustra cómo se conecta Winsock al entorno del protocolo TCP/IP.
**********2_008.tif**********
<Pie figura>**Figura 2.8.** La interfaz Winsock.
<Nivel 1>Distinguir entre seguridad y topologías
<Cuerpo texto>La topología de seguridad de red define el diseño y la implementación desde el punto de vista de la seguridad. Al contrario que en la topología de red, en este caso nos centramos en los métodos de acceso, la seguridad y las tecnologías utilizadas. La topología de seguridad abarca cuatro áreas esenciales:
<Sep-med>* Objetivos de diseño.
* Zonas de seguridad.
* Tecnologías.
* Requisitos de empresa.
<Nivel 2>Establecer los objetivos de diseño
<Cuerpo texto>Cuando establezca los objetivos de diseño para la topología de seguridad, debe plantearse cuestiones de confidencialidad, integridad, disponibilidad y responsabilidad. Las cuatro serán temas transversales en este libro ya que se aplican a diferentes áreas. Abordarlosen la primera fase del diseño de la red le ayudará a establecer una seguridad más estricta. En algunas ocasiones, encontrará que se hace referencia a confidencialidad, integridad y disponibilidad como el CID de la seguridad de red, pero el componente de la responsabilidad es también importante

(los objetivos de diseño deben identificar quién es responsable de los distintos aspectos de la seguridad informática). Las siguientes secciones presentan estos cuatro componentes de seguridad.
<Nivel 3>Confidencialidad
<Cuerpo texto>Cumplir el objetivo de la confidencialidad es evitar o minimizar el acceso no autorizado y la divulgación de datos e información. En muchos casos, las leyes y regulaciones requieren información específica sobre la confidencialidad. Por ejemplo, los registros de la Seguridad Social, las nóminas, los informes de los empleados, los historiales médicos y la información corporativa son activos muy valiosos. Esta información podría conllevar responsabilidades o situaciones embarazosas si caen en manos equivocadas. Durante los últimos años, se han dado algunos casos en los que se han publicado en Internet números de cuentas bancarias y tarjetas de crédito. El coste de este tipo de infracciones de la confidencialidad exceden con mucho las pérdidas reales del mal uso de esta información.
<Nota>**Truco:** La confidencialidad implica asegurar que los datos esperados mantengan su privacidad con el objetivo de que solo los vean aquellos que deberían verlos. La confidencialidad se aplica a través de la autenticación y los controles de acceso.
<Cuerpo texto>Si aborda las cuestiones de confidencialidad en el primer momento de la fase de diseño, aclarará ,desde el principio, los pasos que se deben llevar a cabo para minimizar la exposición.
<Nivel 3>Integridad
<Cuerpo texto>Cumplir el objetivo de la integridad conlleva asegurar que los datos con los que está trabajando son los correctos. La integridad de la información es esencial para una topología segura. Las empresas trabajan y toman decisiones usando los datos que tienen a su disposición. Si esta información no es precisa o la han manipulado personas no autorizadas, las consecuencias podrían ser devastadoras.
Imagine que un distrito escolar pierde todas las nóminas y expedientes de los empleados. Cuando el problema salga a la luz, no habrá más remedio que enviar solicitudes y formularios a todos los trabajadores, preguntándoles cuánto tiempo habían trabajado en ese distrito y cuál era su salario. La integridad se pone en peligro porque los datos son vulnerables y se pueden perder.
<Nota>**Truco:** Puede pensar en la integridad como el nivel de confidencialidad que se supone que tienen que tener los datos, que no deben estar manipulados ni modificados. Auténticos, completos y fiables son algunos de los términos que se suelen utilizar para describir la integridad en términos de datos.
<Nivel 3>Disponibilidad
<Cuerpo texto>Para cumplir el objetivo de la disponibilidad, debe proteger los datos y evitar que se pierdan. La información a la que no se puede acceder tiene poco valor. Si un contratiempo o ataque hace que se bloquee el servidor principal o la base de datos, la información no estará disponible para los que la necesitan. Esto es algo que puede provocar estragos en una empresa. Su trabajo es proporcionar la máxima disponibilidad a los usuarios, a la vez que asegura la integridad y la confidencialidad. La parte más difícil de este proceso es determinar el equilibrio entre estos tres aspectos con el fin de ofrecer una seguridad aceptable para la información y recursos de la empresa.
<Nota>**Truco:** La clave para la disponibilidad es que los datos deben estar dispuestos siempre que sean necesarios y que solo pueden acceder a ellos quienes los necesitan.
<Nivel 3>Responsabilidad
<Cuerpo texto>El último objetivo de diseño, y que en algunas ocasiones se pasa por alto, hace referencia a la responsabilidad. Muchos de los recursos que utiliza una empresa se comparten entre departamentos e individuos. Si se produce un error o incidente, ¿quién es el responsable de solucionarlo? ¿Quién determina si la información es correcta?
Es una buena idea asegurarse de quién tiene los datos o quién es el responsable de corroborar que son precisos. También debería haber un seguimiento y control de las modificaciones de datos para detectarlos y repararlos en caso de pérdida o daño. La mayoría de sistemas registran y almacenan los accesos en las actividades del sistema y la manipulación de datos. Además, proporcionan informes sobre los problemas que surgen.
**********INICIO DE NOTA**********
<Nivel 3>Calcular la disponibilidad
<Nota>La disponibilidad se suele expresar en términos de tiempo activo. La disponibilidad alta alcanza un tiempo activo de 99,9999% a lo largo del año (24 horas al día, 7 días a la semana, 365 días al año). Calcule durante cuánto tiempo los datosno han estado disponibles a lo largo de un año con los siguientes porcentajes de disponibilidad. Por ejemplo, con un tiempo activo del 98%, hay un 2% de inactividad de 525,6 minutos al año. Esto significa que los datos no estuvieron disponibles durante 10,512 minutos o 7⅓ días. Intente calcular lo siguiente:
<Sep-med>1. 99%
2. 99,9%
3. 99,99%
4. 99,999%
5. 99,9999%
<Nota>Puede que el incremento parezca pequeño pero a lo largo del año representa una cifra significativa en lo que respecta a la cantidad de tiempo que los datos no están disponibles. Respuestas: (1.) 5,256 minutos, más de 87 horas o 3,5 días; (2.) 525 minutos, o poco menos de 9 horas; (3.) 52,56 minutos; (4.) 5,25 minutos, y (5.) medio minuto, aproximadamente.
**********FIN DE NOTA**********
<Nivel 2>Crear zonas de seguridad
<Cuerpo texto>Con el tiempo, las redes es posible que alcancen una gran complejidad. Lo que empezó como un grupo de ordenadores compartiendo recursos puede crecer con gran rapidez y convertirse en algo parecido a una pesadilla para un electricista. En ocasiones, puede parecer que las redes cobran vida. Es frecuente que una red tenga

conexiones entre departamentos, compañías, países y acceso público usando rutas de comunicación privadas y a través de Internet.
No todos los miembros de la red necesitan acceder a todos los activos de la red. El término zona de seguridad describe los métodos de diseño que aíslan sistemas de otros sistemas o redes. Se pueden aislar redes utilizando hardware y software. Un enrutador es un buen ejemplo de solución con hardware.Para ello, configure algunas máquinas en la red con el fin de que haya ciertos intervalos entre direcciones y que otras aparezcan en un rango diferente. Esta separación hace que las redes sean invisibles entre sí, a menos que un enrutador las conecte. Algunos de los conmutadores de datos más actuales también le permiten dividir las redes en sistemas más pequeños o zonas privadas.
Cuando se estudian las zonas de seguridad en una red, resulta muy útil pensar que se trata de habitaciones. En su casa u oficina, puede tener habitaciones a las que no pueda entrar nadie y otras a las que el acceso esté limitado a personas específicas en determinados casos. Establecer zonas de seguridad en una red es un proceso similar: Estas le permiten aislar sistemas de usuarios no autorizados. A continuación, encontrará las cuatro zonas de seguridad más frecuentes:
<Sep-med>* Internet.
* Intranet.
* Extranet.
* DMZ (*Demilitarized Zone*, Zona desmilitarizada).
**********INICIO DE NOTA**********
<Nivel 3>La responsabilidad son más que palabras
<Cuerpo texto>La responsabilidad, como el sentido común, se aplica a todos los aspectos de las tecnologías de la información. Hace varios años, una empresa que dependía de datos que no podían reconstruirse escribió scripts de Shell para realizar copias de seguridad por la mañana temprano, cuando los host estaban menos ocupados. Se les pedía a los operadores de estas máquinas que insertaran un dispositivo en la unidad alrededor de media noche y que volvieran a comprobarlo sobre las 3:00 de la madrugada para asegurarse de que se había imprimido un comprobante en el que se indicaba que la tarea había concluido. Si el papel aparecía, extraían el dispositivo y lo almacenaban. De lo contrario, llamaban al servicio de soporte técnico.
Una mañana se produjo el inevitable colapso del disco duro y se le pidió a un técnico especializado en tecnologías de la información que lo cambiara. El técnico sustituyó el disco duro y pidió las copias de seguridad más recientes. Para su desgracia, los datos tenían dos años de antigüedad. La máquina se estropeó antes de que se realizara la copia de seguridad, pero el técnico pensó que las probabilidades de remontarse dos años atrás eran muy improbables. Sin dar crédito, pidió la copia de seguridad del día anterior y descubrió que los datos también tenían dos años de antigüedad. Empezando a preocuparse, buscó a la última operadora del host y le preguntó si había realizado las copias de seguridad. Esta le aseguró que sí y que colocaba las cintas y las sacaba tan pronto como se imprimía el comprobante. Al preguntarle por qué los datos eran tan antiguos, ella aseguró que podía probar su historia porque también había guardado los comprobantes que aparecían en la impresora cada día. Los buscó y se los dio. Todos los documentos decían lo mismo: el dispositivo de la unidad estaba protegido contra escritura.
¿Dónde recae la responsabilidad de esta historia real? La operadora siguió con atención las instrucciones que le dieron y cumplía el proceso para realizar las copias de seguridad de la información de la empresa cada noche. Ella pensó que el hecho de que la unidad estuviera protegida era algo bueno. Se descubrió que todos los host estaban imprimiendo el mismo mensaje, pero la operadora carecía de la formación necesaria para detectar el problema, dejando a la compañía sin copias de seguridad durante dos años.
El problema no residía en la operadora sino en la formación que recibió. Si le hubieran enseñado el aspecto que deberían presentar los informes correctos e incorrectos, los datos nunca se habrían perdido.
**********FIN DE NOTA**********
<Cuerpo texto>Las siguientes secciones identifican las topologías utilizadas para crear y diseñar zonas de seguridad con el propósito de ofrecer mayor protección. Internet se ha convertido en una gran ayuda a nivel individual y empresarial, pero también supone un desafío en términos de seguridad. Al implementar redes Intranet, Extranet y DMZ, puede crear un entorno bastante seguro para su empresa.
<Nivel 3>Internet
<Cuerpo texto>Internet es una red global que conecta ordenadores y redes individuales. Puede utilizarla cualquiera que acceda a un portal de Internet o a un ISP (*Internet Service Provider*, Proveedor de acceso a Internet). En este entorno, debería tener un bajo nivel de confianza en las personas que utilizan Internet. Siempre tendría que asumir que los que visiten su sitio Web pueden ir con malas intenciones. Es posible que quieran comprar su producto o contratar su empresa o que quieran bloquear sus servidores.
De forma externa, no tiene forma de saberlo hasta que no controle sus acciones. Debido a que Internet conlleva un alto nivel de anonimato, siempre debe salvaguardar sus datos con precauciones extremas.
La figura 2.9 ilustra una red de Internet y sus conexiones.
**********2_009.tif**********
<Pie figura>**Figura 2.9.** Típica conexión LAN a Internet.
<Nota>**Truco:** En algunas ocasiones, los datos que da la red pueden ser tan problemáticos como los que entran en ella. Comprobar la información que ofrece la red para buscar signos de tráfico malicioso es un campo de la seguridad informática bastante novedoso y se conoce como extrusión.
<Nivel 3>Intranet
<Cuerpo texto>Las Intranet son redes privadas implementadas y mantenidas por una empresa individual o una organización. Imagine que Intranet es una red de Interneta la que su compañía no permite entrar; es interna y su acceso está limitado a los sistemas que forman parte de la red. Las Intranet usan las mismas tecnologías que se emplean para Internet. Pueden conectarse a Internet pero no pueden acceder los usuarios que no están autorizados y

que no formen parte de ellas. El usuario anónimo de Internet es, en cambio, un usuario autorizado de Intranet. El acceso a Intranet está garantizado a personas de confianza dentro de la red corporativa o a aquellos que estén en localizaciones remotas.
La figura 2.10 muestra una red Intranet.
**********2_010.tif**********
<Pie figura>**Figura 2.10.** Ejemplo de red Intranet.
<Nivel 3>Extranet
<Cuerpo texto>Las Extranet amplían las Intranet con el fin de incluir conexiones externas a socios. Éstos pueden ser vendedores, proveedores o terceros similares que necesiten acceder a sus datos por razones legítimas. Una Extranet le permite conectar con un socio a través de una red privada o una conexión usando un canal de comunicación seguro a través de Internet. Las conexiones Extranet implican conexiones entre organizaciones fiables.
Puede observar un ejemplo de Extranet en la figura 2.11. Tenga en cuenta que esta red proporciona una conexión entre dos organizaciones y que puede realizarse a través de Internet. En ese caso, estas redes utilizarían un protocolo de túnel para conseguir una conexión segura.
**********2_011.tif**********
<Pie figura>**Figura 2.11.** Típica Extranet entre dos organizaciones.
<Nivel 3>Zona desmilitarizada
<Cuerpo texto>Una DMZ es un área en la que puede colocar un servidor público para que accedan personas que, de otra manera, no serían fiables. Al aislar un servidor en una DMZ, puede ocultar o eliminar el acceso a otras áreas de su red y seguir entrando a su servidor usando su red. Sin embargo, otros no tendrán la posibilidad de acceder a más recursos. Puede conseguirlo usando cortafuegos para aislar su red.
Cuando establece una DMZ, asume que la persona que accede al recurso no tiene por qué ser alguien a quien confiaría otra información. La figura 2.12 muestra un servidor en una DMZ. Observe que el resto de la red no está visible para usuarios externos. Esto reduce el riesgo de intrusión en la red interna.
**********2_012.tif**********
<Pie figura>**Figura 2.12.** Ejemplo de una DMZ típica.
<Nota>**Truco:** Siempre que quiera separar información pública y privada, una DMZ será una opción aceptable.
<Cuerpo texto>La forma más fácil de separar la información pública y privada es usar un cortafuegos que pueda transmitir en tres direcciones:
<Sep-med>* A la red interna.
* Al mundo externo (Internet).
* A la información pública que está compartiendo (la DMZ).
<Cuerpo texto>A partir de ahí, puede decidir a qué lugar va el tráfico. Por ejemplo, el tráfico HTTP se enviaría a la DMZ y el correo electrónico se dirigiría a la red interna.
<Nota>**Truco:** Un host que existe fuera de la DMZ y se abre al público suele llamarse host de bastión. Suele estar constituido por enrutadores y cortafuegos.
<Nivel 3>Diseñar zonas de seguridad
<Cuerpo texto>El diseño de la zona de seguridad es un aspecto importante de la seguridad informática. Puede recurrir a muchos enfoques distintos para conseguir un diseño sólido. Algunas soluciones implican riesgo y dinero. Una opción es crear capas de seguridad para proteger los sistemas de protección menos seguros y, para ello, utilizar NAT (*Network Address Translation*, Traducción de direcciones de red), que le ayuda a ocultar recursos. No obstante, tenga en cuenta que están empezando a aparecer nuevos métodos y herramientas para diseñar redes seguras. Es importante recordar que cuando posea un buen diseño, debería revisarlo teniendo en cuenta lo que ha aprendido sobre riesgos de seguridad.
<Nivel 2>Trabajar con las tecnologías más novedosas
<Cuerpo texto>La tecnología siempre está en continuo cambio. Esto puede ser una ventaja o una desventaja, según el punto de vista que adopte. Muchas de las tecnologías más novedosas están a su disposición para ayudarle a crear sistemas menos vulnerables. Esta sección se centra en las cuatro siguientes:
<Sep-med>* Virtualización.
* VLAN (*Virtual Local Area Networks*, Redes virtuales de área local).
* NAT.
* Tunelado.
<Cuerpo texto>Estas tecnologías le permiten mejorar la seguridad de su red con un pequeño coste adicional.
<Nivel 3>Tecnología de virtualización
<Cuerpo texto>La virtualización es la tecnología de moda, con VMware, uno de los mayores vendedores de esta tecnología, contando el cien por cien de los miembros del prestigioso listado Fortune 100 como parte de su base de clientes. Además de soluciones de propietario, también existen otras de acceso libre. Los ejemplos más conocidos son Xen y VirtualBox.
La tecnología de virtualización le permite ocultar las características de un único dispositivo físico a los usuarios. Básicamente, le permite ejecutar varios elementos en un dispositivo y hacer que aparezcan como si se tratara de entidades independientes. Por ejemplo, un terminal solo puede ejecutar un sistema operativo al mismo tiempo. Usando la virtualización, es posible que ejecute Windows 7 y, además, Fedora, Red Hat, Windows Server 2008, así como otros sistemas operativos dentro de la ventana virtual. El desarrollador informático que trabaja con código puede moverse entre las ventanas, cortando y pegando, si quiere, o haciendo todo aquello que necesite en una máquina, sin tener en marcha cuatro terminales diferentes. Gracias a la virtualización, el terminal puede iniciar varios sistemas operativos, distintas versiones del mismo sistema o múltiples aplicaciones, entre otras cosas.

Solo puede usar la virtualización en un terminal o en un servidor. Un único servidor puede hospedar múltiples máquinas lógicas. Al emplear un servidor que lleve a cabo las funciones de muchos, puede ahorrar costes de forma inmediata en términos de hardware, utilidad e infraestructura, por mencionar algunos.
Por muy maravillosa que parezca la virtualización, puede presentar algunos desafíos desde el punto de vista de la seguridad. Un usuario que entra al sistema podría tener acceso a todo (no solo a su máquina virtual) si pudiera invalidar la protección de la capa física. Cuando se estaba escribiendo este libro, la amenaza de que eso ocurriera era más un rumor que un hecho, pero conforme ha ido creciendo la popularidad de la virtualización, es una apuesta segura que las máquinas virtuales se convertirán en un popular destino de delincuentes en los próximos años.
<Nivel 3>Redes virtuales de área local
<Cuerpo texto>Una red VLAN (*Virtual Local Area Networks*, Redes virtuales de área local) le permite crear grupos de usuarios y sistemas, así como segmentarlos. Esta segmentación hace que pueda ocultar algunas partes de la red y, de ese modo, controlar el acceso. También puede establecer redes VLAN para controlar las rutas que seguirán los datos de un punto a otro. Un VLAN es un buen método para contener el tráfico a determinadas zonas de la red.
<Nota>**Truco:** Piense en VLAN como una red de varios host que actúan como si estuvieran conectados por un cable físico aunque este no exista en realidad.
<Cuerpo texto>En una LAN, los host pueden comunicarse entre sí a través de transmisiones y no se necesitan dispositivos de envío, como enrutadores. Cuando la LAN crece, también lo hace el número de transmisiones. Reduciendo el tamaño de la red LAN y segmentándola en grupos más pequeños (VLAN), disminuye el tamaño de los dominios de transmisión. Las ventajas de hacer esto incluyen la deducción del alcance de las transmisiones, la mejora del rendimiento y la manejabilidad, además de reducir la dependencia en la topología física. No obstante, desde el punto de vista del examen, la ventaja clave es que las redes VLAN pueden incrementar la seguridad permitiendo a los usuarios con niveles de confidencialidad de datos similares realizar una segmentación conjunta.
La figura 2.13 ilustra la creación de tres VLAN en una única red.
**********2_013.tif**********
<Pie figura>**Figura 2.13.** Típica VLAN segmentada.
<Nivel 3>Traducción de direcciones de red
<Cuerpo texto>La NAT crea una oportunidad única para atender la seguridad de una red. En su origen, esta amplió el número de direcciones de Internet disponibles y, en la actualidad, permite a una organización presentar una dirección única de Internet para todas las conexiones informáticas. El servidor NAT proporciona direcciones IP para los host o sistemas de la red y registra el tráfico de entrada y salida.
Una empresa que usa NAT presenta una única conexión de red. Esta puede producirse a través de un enrutador o de un servidor NAT. La única información que puede conseguir un intruso es que la conexión solo tiene una dirección. NAT oculta su red al mundo, haciendo mucho más difícil determinar qué sistemas existen al otro lado del enrutador. Es decir, funciona como un cortafuegos simple y económico para redes pequeñas.. La mayoría de enrutadores son compatibles con NAT.<Nota>**Truco:** Es importante entender que NAT actúa como un proxy entre la red de área local (que puede utilizar direcciones IP privadas) e Internet. Pero no solo puede guardar direcciones IP, sino que también actúa como un cortafuegos.
<Cuerpo texto>La mayoría de implementaciones NAT asignan a host internos números privados de direcciones IP solo para que NAT traduzca y se comunique con el mundo externo.
Los intervalos de direcciones privadas, todas no enrutables, son los siguientes:
<Listados>10.0.0.0–10.255.255.255
172.16.0.0–172.31.255.255
192.168.0.0–192.168.255.255
<Cuerpo texto>La figura 2.14 muestra un enrutador proporcionando servicios NAT a una red. En el enrutador presenta una única dirección para todas las conexiones externas de Internet.
**********2_014.tif**********
<Pie figura>**Figura 2.14.** Típica conexión a Internet para una red local.
<Nota>**Truco:** Además de NAT, también puede utilizar PAT (*Port Address Translation*, Traducción de direcciones de puertos). Mientras que NAT puede utilizar varias direcciones públicas IP, PAT solo utiliza una y comparte el puerto con la red. Debido a que está empleando un único puerto, PAT es mucho más limitada y solo se suele usar en redes pequeñas. Un ejemplo de implementación PAT es la conexión compartida a Internet de Microsoft.
<Nota>**Nota:** El direccionamiento IP es un tema del examen Network+ y no de Security+, pero CompTIA espera que tenga un conocimiento básico. Además de entender el concepto que se desprende de NAT, debería saber que la división en subredes es el modo en que se fragmentan las redes. Las RFC (*Requests for Comments*, Solicitud para comentarios) 1466 y 1918 detallan la división en subredes. Puede encontrarlas en http://www.faqs.org/rfcs/.
<Nivel 3>Tunelado
<Cuerpo texto>El tunelado hace referencia a la creación de una conexión virtual establecida entre dos sistemas o redes. El túnel se crea entre los extremos y encapsula los datos mediante un protocolo en el que ambos se han puesto de acuerdo para la transmisión. En la mayoría de túneles, los datos que pasan a través de este aparecen en el otro lado como parte de la red.
Los protocolos de túnel suelen incluir seguridad de datos, así como cifrado. Han aparecido muchos estándares conocidos para el tunelado, el ejemplo más popular es L2TP (*Layer 2 Tunneling Protocol*, Protocolo de túnel de capa dos).
<Nota>**Truco:** El túnel envía datos privados a través de una red pública y los coloca (los encapsula) en otros paquetes. La mayoría de túneles son VPN (*Virtual Private Networks*, Redes privadas virtuales).
<Cuerpo texto>La figura 2.15 muestra una conexión entre dos redes a través de Internet. Para cada extremo de la red hay una conexión única.

**********2_015.tif**********
<Pie figura>**Figura 2.15.** Típico ejemplo de túnel.
<Nivel 3>Telefonía
<Cuerpo texto>Cuando se combinan la tecnología telefónica y la informática se obtiene la telefonía. Una infracción en su infraestructura de telefonía es tan devastadora como cualquier otra violación y puede derivar en la pérdida de datos valiosos.
Debido al éxodo de las líneas de tierra a VoIP (*Voice over IP*, Voz sobre IP) para que las compañías ahorren, es crucial que se le dé la misma importancia a esta parte de la red que a cualquier otra. VoIP puede ser curioseada con herramientas como Cain & Abel (http://www.oxid.it/) y es susceptible de ataques DoS (*Denial of Service*, Denegación de servicio) ya que depende de UDP. No se debe olvidar la interrupción con VoIP en los casos en que se bloquea la red de datos y, además, se pierde la telefonía.
Como ejemplo de la información que tiene a su disposición, SecureLogix comercializa un cortafuegos de voz (http://www.securelogix.com/ip-telephony-security.html) y Cisco ha publicado un informe titulado " IP Telephony Security in Depth" (Seguridad de la tecnología IP en detalle) que encontrará en http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf.
<Nota>**Nota:** Desde el punto de vista de la seguridad, el mayor problema que presenta VoIP y los datos que están en la misma línea es que ambos son vulnerables si se produce un ataque PBX (*Private Branch Exchange*, Central de conmutación privada). Para más información sobre PBX, diríjase a http://www.pbxinfo.com/.
<Nivel 2>Trabajar con los requisitos de empresa
<Cuerpo texto>El componente final del diseño de seguridad es trabajar con los requisitos de empresa. Varios capítulos de este libro se centran en entender los requisitos de empresa y en el trabajo con las políticas y estándares. En este caso, solo debe saber que no hay una solución mágica que encaje en todas las situaciones de forma tan sencilla como en las otras tres áreas (objetivos de diseño, zonas de seguridad y tecnología), ya que cada compañía tendrá distintos requisitos empresariales, incluyendo un nivel de riesgo diferente que están dispuestos a aceptar y distintas regulaciones a las que deben adherirse.
<Nivel 1>Seguridad de la infraestructura
<Cuerpo texto>Como su nombre indica una infraestructura es la base de todo el trabajo que se produce en una organización. La seguridad de la infraestructura trata los aspectos más básicos del flujo de información y del funcionamiento en la red y los sistemas. Cuando se habla de infraestructura, tenga en cuenta que se incluyen los servidores, las redes, los dispositivos de red, los terminales y los procesos establecidos para facilitar el trabajo.
Con el objetivo de evaluar la seguridad de su infraestructura, debe examinar el hardware y sus características, así como el software y sus particularidades. Cada vez que añade un dispositivo, modifica configuraciones o cambia tecnologías, por lo que puede estar alterando las capacidades de seguridad fundamentales de su red. Una cadena no es más fuerte que su eslabón más débil, también se suele decir que una red no es más segura que su nodo más frágil.
Las redes están vinculadas a través de Internet y otras tecnologías de red, de este modo, se vuelven vulnerables a numerosos ataques. El trabajo de un profesional de la seguridad es eliminar las amenazas obvias, anticipar cuál será el próximo asalto que se puede producir en su infraestructura y estar preparado para neutralizarlo antes de que tenga lugar.
Las siguientes secciones describen los componentes de hardware y software que configuran una red.
<Nivel 2>Trabajar con los componentes de hardware
<Cuerpo texto>Los componentes de hardware de red incluyen dispositivos físicos como enrutadores, servidores, cortafuegos, terminales y conmutadores. La figura 2.16 representa una típica infraestructura de red y algunos de sus componentes de hardware más comunes en el entorno. Desde el punto de vista de la seguridad, esta infraestructura es mucho más que la suma de todas sus partes. Debe evaluar la red desde la perspectiva de todos y cada uno de los dispositivos que la componen. La complejidad de la mayoría de las redes hace que asegurarlas sea complicado en extremo. Para proporcionar una seguridad razonable, debe evaluar cada dispositivo y, así, determinar sus fortalezas y debilidades.
**********2_016.tif**********
<Pie figura>**Figura 2.16.** Típica infraestructura de red.
<Cuerpo texto>Fíjese en que en la anterior figura la red que evaluará tiene conexiones a Internet. Estas exponen a su red al mayor número de amenazas, las cuales pueden proceder de casi cualquier parte del mundo.
**********INICIO DE NOTA**********
<Nivel 3>Actualizar la lista de infraestructura
<Nota>Como administrador tiene que tratar con una variedad de dispositivos cada día. No solo tiene la obligación de atender a las necesidades de los servidores, sino que además debe mantener el acceso a Internet, gestionar multitud de usuarios y terminales, así como conseguir que todo funcione sin problemas. Puede tener cortafuegos tras cortafuegos en acción, pero si permite a un vendedor conectarse con una protección mínima, esa conexión se convertirá en la línea base de la seguridad.
Por lo tanto, llevar un seguimiento del hardware de la empresa es una tarea muy importante y, por ello, debería hacer un inventario de su red y configurar una lista de infraestructuras. Si ya lo ha hecho, esta es una ocasión ideal para actualizarla. Cuando lo tenga, tome nota de todos los dispositivos que están conectados a su red, ya sea de forma continuada o intermitente. A continuación, encontrará una serie de preguntas que debe responder:
<Sep-med>1. ¿Cuántos servidores hay? ¿Cuál es la función de cada uno de ellos y qué nivel de seguridad se les aplica?
2. ¿Cuántos terminales hay? ¿Qué sistema operativo utilizan? ¿Cómo se conecta a la red (cableado, red inalámbrica, marcado)?

3. ¿Cómo abandonan la red los datos (enrutadores, puertas de enlace)? ¿Cuál es la seguridad de cada uno de estos dispositivos? ¿Están impidiendo el tráfico los cortafuegos u otros dispositivos?
4. ¿Qué más dispositivos hay conectados a la red (por ejemplo, módems) que puedan emplearse para acceder a ella?

<Nota>Con toda la honestidad, esta información ya debería estar registrada y disponible. Aunque, si su empresa es como la mayoría, la información no existirá y los dispositivos se añadirán cuando vayan siendo necesarios, con la intención de crear la documentación más adelante. No hay mejor ocasión para crearla. Sea consciente de la actitud que muchos parecen tener: "¡Eso no nos pasará a nosotros!" Debe estar preparado para gestionarla explicando que sí puede pasarles y que hay que hacer todo lo posible para evitarlo.
**********FIN DE NOTA**********

<Nivel 2>Trabajar con componentes de software

<Cuerpo texto>El hardware existe para ejecutar el software. A su vez, el software está ideado para hacer que los componentes del hardware sean fáciles de configurar. Sin embargo, en cierta medida, el software también puede hacer que el hardware sea susceptible de desvío.

La infraestructura de red ilustrada en la figura 2.1 incluye servidores, terminales ejecutando sistemas operativos, un enrutador, un cortafuegos (puede haber algunos que se ejecuten como aplicaciones en servidores) y dispositivos específicos que tienen sus propios programas de comunicación y control. Esta situación deja a las redes expuestas a posibles ataques y problemas de seguridad, ya que muchos de estos sistemas funcionan de forma independiente.

Numerosas grandes empresas han creado un área exclusiva para la supervisión de la red y el control administrativo de los sistemas. Esta centralización le permite ver un esquema general de la red y tomar medidas teniendo en cuenta varios sistemas o recursos de red si se produce un ataque. Como área centralizada se llama NOC (*Network Operations Center*, Centro de operación de redes). Usar un NOC le facilita la observación del desarrollo de un ataque y la adopción de medidas defensivas. Por desgracia, este no se encuentra al alcance de gran parte de las pequeñas y medianas empresas. Los NOC son caros y requieren gran soporte técnico, factores que van más allá de la economía o la escala de todos, salvo de las grandes empresas. El trabajo no acaba una vez que se desarrolla y se implementa un NOC, este debe evaluarse de forma constante para realizar las modificaciones pertinentes.

<Nota>**Nota:** Si su empresa no cuenta con un profesional dedicado a la seguridad, pero necesita implementar medidas de este tipo, un modo es contratar a un MSSP (*Managed Security Service Provider*, Proveedor de servicios de seguridad administrada). Este ofrece servicios de seguridad general a pequeñas empresas y puede resultar más beneficioso que incluir un individuo dedicado en nómina.
**********INICIO DE NOTA**********

<Nivel 3>NOC de AT&T Wireless

<Nota>AT&T Wireless mantiene un NOC enorme para cada uno de los centros móviles que gestiona. Dichos centros proporcionan una supervisión 24 horas, 7 días a la semana en tiempo real para todos los dispositivos de la red móvil e informática que administran. Los operadores del NOC pueden alcanzar y tocar cualquier dispositivo de la red para configurarlo, repararlo y resolver problemas. Un solo NOC tiene docenas de personas trabajando a contrarreloj para mantener la red en condiciones óptimas. Cuando se bloquea algún centro NOC, se impide el servicio normal de telefonía móvil de toda la región. Como puede imaginar, esto supone un gasto increíble y la empresa no permitirá que suceda muy a menudo. En EE. UU. hay numerosas instalaciones NOC y una región puede suplir a otra si el centro está inoperativo de forma temporal.
**********FIN DE NOTA**********

<Nivel 1>Dispositivos de la infraestructura de red

<Cuerpo texto>Conectar todos estos componentes requiere dispositivos físicos. Las grandes corporaciones multinacionales, así como las pequeñas y medianas empresas están construyendo redes de enorme complejidad y sofisticación. Estas funcionan utilizando kilómetros de tecnologías de cableado e inalámbricas. Si la totalidad de la red está basada en cableado y fibra o, por el contrario, es inalámbrica por completo, el método para transmitir datos de un lugar a otro abre vulnerabilidades y oportunidades para la explotación. Las debilidades aparecen siempre que exista la posibilidad de interceptar información de los medios.

Los dispositivos que se describen brevemente a continuación son los componentes que encontrará en una red de forma habitual.

<Nota>**Nota:** Muchos dispositivos de red contienen *firmware* con el que puede interactuar durante la configuración. En cuanto a la seguridad, debe autenticarse para realizar modificaciones en la configuración y, en un inicio, tiene que utilizar la cuenta/s predeterminada/s. No olvide cambiar la contraseña predeterminada tras la instalación de un dispositivo en la red. De lo contrario, está dejándolo abierto a cualquiera que haya accedido al hardware y podrá entrar usando la contraseña de fábrica.

<Nivel 2>Cortafuegos

<Cuerpo texto>Los cortafuegos son una de las primeras líneas de defensa en una red. Hay distintos tipos y pueden ser sistemas independientes o estar incluidos en otros dispositivos, como enrutadores o servidores. Podrá observar que hay opciones de cortafuegos que se comercializan solo como hardware y otras solo como software. No obstante, muchos cortafuegos están formados por un software complementario disponible para servidores o terminales.

<Nota>**Nota:** Aunque algunas soluciones se vendan como "solo hardware", este sigue necesitando algún tipo de software. Puede que esté reforzado, que se encuentre en la memoria ROM para evitar alteraciones y que pueda personalizarlo. Pero el software debe estar presente en cualquier caso.

<Cuerpo texto>El propósito esencial de un cortafuegos es aislar una red de otra. Comienzan a estar disponibles como aparatos. Esto significa que se instala como el dispositivo primario que separa dos redes. Se trata de dispositivos independientes que funcionan de forma autosuficiente en gran medida y, por lo tanto, requieren un mantenimiento menor que un producto basado en servidor.

<Nota>**Truco:** Para entender el concepto de cortafuegos, es útil conocer la procedencia del término. Hace tiempo, las viviendas solían construirse tan cerca unas de otras que si se producía un incendio en una, podría destruir con facilidad un bloque o muchos más antes de que pudiera extinguirse. Para disminuir el riesgo de que sucediera esto, se construían cortafuegos entre los edificios. Estos sistemas de protección consistían en enormes muros de ladrillo que separaban los edificios y mantenían el fuego confinado en uno de los lados. El mismo concepto de restricción y contención se aplica a los cortafuegos virtuales. El tráfico del mundo externo golpea al cortafuegos y no se le permite entrar a la red a menos que se trate de un invitado.
<Cuerpo texto>El cortafuegos que aparece en la figura 2.17 limita el acceso a las redes externas de forma efectiva y, al mismo tiempo, permite a los usuarios internos de la red acceder a recursos foráneos. El cortafuegos de esta ilustración también lleva a cabo funciones proxy, que trataremos más adelante.
**********2_017.tif**********
<Pie figura>**Figura 2.17.** Un cortafuegos proxy que bloquea el acceso a redes externas.
<Cuerpo texto>Los cortafuegos funcionan como alguno o algunos de los siguientes:
<Sep-med>* Filtrado de paquetes.
* Cortafuegos proxy.
* Inspección con estado.
<Nota>**Truco:** Aunque los cortafuegos se suelen asociar al tráfico externo, puede colocarlos en cualquier parte. Por ejemplo, si quiere aislar una parte de su red interna, puede colocar un cortafuegos entre ambos lados.
<Nivel 3>Filtrado de paquetes
<Cuerpo texto>Un cortafuegos que actúa como un filtrado de paquetes deja pasar el tráfico de una dirección específica o lo bloquea basándose en el tipo de aplicación. Dicho filtrado no analiza su contenido, únicamente decide si el paquete pasa o no según su información de direccionamiento. Por ejemplo, un filtrado de paquetes puede permitir el tráfico Web en el puerto 80 y bloquear el tráfico Telnet en el puerto 23. Este tipo de filtrado se incluye en muchos enrutadores. Si la solicitud de un paquete recibido quiere acceder a un puerto no autorizado, el filtro puede rechazarla o limitarse a ignorarla. Muchos filtrados de paquetes también especifican qué direcciones IP pueden solicitar determinados puertos y permitir o denegar el acceso dependiendo de la configuración de seguridad del cortafuegos.
El filtrado de paquetes está creciendo en cuanto a sofisticación y capacidad se refiere. Un cortafuegos de este tipo permite cualquier tráfico que califique como aceptable. Por ejemplo, si quiere que los usuarios Web accedan a su sitio, puede configurar el cortafuegos de filtrado de paquetes para permitir que entren datos en el puerto 80. Si todas las redes fueran iguales, los cortafuegos tendrían puertos configurados de fábrica, pero las redes varían y, por ello, los cortafuegos no incluyen esta opción.
**********INICIO DE NOTA**********
<Nivel 3>Decidir qué tráfico se permite
<Nota>Como administrador tiene que analizar su red y decidir a qué tráfico se le permitirá pasar por el cortafuegos. ¿Qué tráfico va a permitir? ¿A cuál le bloqueará el acceso?
A continuación, encontrará una lista en la que solo aparecen los puertos TCP más frecuentes (véase la tabla 2.3). Utilice las casillas para determinar si permite o no el tráfico de los datos que utilizan un puerto específico a través del cortafuegos.
<Pie figura>**Tabla 2.3.** Puertos TCP más frecuentes.
**********NOTA AL MAQUETADOR SUSTITUIR LA X POR EL ELEMENTO DE LA TABLA DEL ORIGINAL**********

<Tablas>

Número de puerto TCP	**Servicio**		**Sí**	**No**
20	FTP (canal de datos)	X	X	
21	FTP (canal de control)	X	X	
23	Telnet	X	X	
25	SMTP	X	X	
49	TACACS para servicio de autenticación		X	X
80	HTTP (utilizado para World Wide Web)		X	X
110	POP3	X	X	
119	NNTP	X	X	
137, 138, y 139	NetBIOS para servicio de sesión		X	X
143	IMAP	X	X	
389	LDAP	X	X	
443	HTTPS (utilizado para conexiones Web seguras)		X	X
636	LDAP (SSL)	X	X	

**********FIN DE NOTA**********
<Nivel 3>Cortafuegos proxy
<Cuerpo texto>Piense en un cortafuegos proxy como si se tratara de un intermediario entre su red y cualquier otra. Este se utiliza para procesar las solicitudes procedentes de una red externa. Con este objetivo, analiza los datos y toma decisiones basándose en algunas reglas para determinar si se reenvía o se rechaza la solicitud. El proxy intercepta todos los paquetes y los vuelve a procesar para uso interno. Este proceso incluye ocultar las direcciones IP.
<Nota>**Truco:** Cuando considere el concepto de ocultar direcciones IP, recuerde lo que aprendió sobre NAT.
<Cuerpo texto>El cortafuegos proxy proporciona una mejor seguridad que el filtrado de paquetes debido al incremento de capacidad que ofrece este tipo de cortafuegos. Las solicitudes de los usuarios de una red interna se distribuyen a través del proxy. Este, a su vez, vuelve a empaquetar las solicitudes y las envía. De este modo, aísla al

usuario de redes externas. El proxy también ofrece almacenamiento en cache, suponiendo que se vuelva a realizar la misma solicitud, con lo que incrementa la eficacia de los datos entregados.
En general, un cortafuegos proxy utiliza dos NIC. Este tipo de dispositivo se conoce como cortafuegos de doble alojamiento. Una de las tarjetas se conecta a la red externa y otra a la interna. El software del proxy gestiona las conexiones entre las dos NIC. Esta configuración segrega las dos redes y ofrece una seguridad añadida. La figura 2.8 ilustra un cortafuegos de doble alojamiento separando dos redes.
**********2_018.tif**********
<Pie figura>**Figura 2.18.** Cortafuegos de doble alojamiento separando dos redes.
**********INICIO DE NOTA**********
<Nivel 3>Cortafuegos de doble alojamiento
<Cuerpo texto>Imagine que es el administrador de una red pequeña y que stá instalando un nuevo servidor de seguridad. Cuando ha concluido la instalación, observa que la red no parece estar distribuyendo el tráfico a través del cortafuegos y que las solicitudes de entrada no se están bloqueando. Esta situación presenta un problema de seguridad para la red, ya que ha detectado tráfico inusual en varias ocasiones.
La solución más probable para este problema es que el servidor ofrezca la posibilidad de usar reenvíos IP en un servidor de doble alojamiento. El reenvío IP omite el cortafuegos y utiliza el servidor como enrutador. Aunque se aíslen las dos redes con eficacia, el nuevo enrutador está haciendo bien su trabajo y está redirigiendo el tráfico IP. Por último, tendrá que verificar que el reenvío IP y los servicios de enrutamiento no se están ejecutando en este servidor.
**********FIN DE NOTA**********
<Nota>**Truco:** Siempre que configure un sistema con más de una dirección IP, puede decirse que se trata de un sistema con múltiples alojamientos.
<Cuerpo texto>La función proxy puede producirse en cualquier nivel de aplicación o del circuito.
Dicha función, a nivel de aplicación, lee los comandos individuales del protocolo que se está sirviendo. Este tipo de servidor es avanzado y debe conocer las reglas y capacidades del protocolo utilizado. Una implementación de estas características tiene que conocer la diferencia existente entre las operaciones GET y PUT, por ejemplo, y manejar reglas que especifiquen su ejecución. Un proxy a nivel de circuito crea un itinerario entre el cliente y el servidor y no se encarga del contenido de los paquetes que se están procesando.
Por otro lado, es aconsejable que solo exista un servidor proxy a nivel de aplicación para cada protocolo admitido. Muchos servidores de este tipo también proporcionan una autoría y responsabilidad completas, así como otra información de uso que no se guardaría en servidor proxy a nivel de circuito.
<Nivel 3>Inspección con estado
<Cuerpo texto>La última sección sobre los cortafuegos se centra en el concepto de inspección con estado. Para entender la terminología, resulta útil saber con antelación a qué nos referimos con "sin estado".
Los cortafuegos sin estado toman decisiones basándose en los datos entrantes, por ejemplo, en el paquete, y no en decisiones complejas.
La inspección con estado también se conoce como filtrado de paquetes con estado. La mayoría de los dispositivos empleados en las redes no almacenan un seguimiento de cómo se dirige o utiliza la información. Cuando se pasa un paquete, este y su ruta se olvidan. En la inspección con estado (o filtrado de paquetes con estado), se guardan registros usando una tabla de estado que almacena todos los canales de comunicación. Las inspecciones con estado se producen en todos los niveles de la red y proporcionan seguridad adicional, especialmente en los protocolos sin conexión como UDP y ICMP. Esto añade complejidad al proceso. Los ataque DoS (*Denial-of-Service*, Denegación de servicio) suponen un desafío porque se utilizan técnicas de desbordamiento para desviar la tabla de estado y provocar que el cortafuegos se desactive o se reinicie.
<Nota>**Truco:** Para el examen, recuerde que el filtrado de paquetes no tiene inteligencia real. Este permite que los datos pasen a través del puerto si está configurado y, de lo contrario, lo desecha sin examinarlos. Sin embargo, el filtrado de paquetes con estado tiene inteligencia y almacena el registro de todos los canales de comunicación.
<Nivel 2>Concentradores
<Cuerpo texto>Uno de los dispositivos más simples en una red es el concentrador. Aunque es posible cargar un software para crear un concentrador gestionado, en realidad, un concentrador no es otra cosa que un dispositivo que permite comunicarse con muchos host mediante el uso de puertos físicos. El tráfico de difusión traspasa el concentrador y todos los datos recibidos a través de un puerto se envían a los demás. Esta organización crea un entorno extremadamente inseguro si un intruso se adhiere al concentrador y empieza a interceptar datos.
<Nota>**Nota:** Las difusiones son mensajes que se envían desde un sistema único a toda la red. La multidifusión envía un mensaje a varias direcciones. La unidifusión está orientada a un único sistema.
<Cuerpo texto>Algunos de los concentradores más caros le permiten habilitar seguridad de puertos. Si cambia la dirección MAC, el concentrador deshabilita el puerto. La seguridad de puertos incrementa el nivel de protección de la red LAN, pero también puede aumentar el volumen de trabajo si re configurar el entorno con frecuencia.
<Nota>**Truco:** Para el examen, piense en los concentradores como dispositivos LAN inseguros de forma predeterminada que deberían sustituirse por conmutadores por cuestiones de seguridad y para incrementar el rendimiento.
<Nivel 2>Módems
<Cuerpo texto>Un módem es un dispositivo hardware que conecta las señales digitales de un ordenador con un línea de teléfono analógica. Este permite que las señales se transmitan a mayores distancias de lo que suele ser posible. La palabra módem es un combinación de los términos modulador y demodulador, dos funciones que se producen durante la transmisión.

Estos dispositivos presentan una serie de desafíos únicos desde la perspectiva de la seguridad. La mayoría de ellos responden a cualquier llamada cuando están conectados a una línea exterior. Cuando el aparato receptor contesta el teléfono, suele sincronizarse con el dispositivo de llamada y realizar una conexión. Un módem, cuando se conecta de forma indebida a una red, puede permitir acceso instantáneo inseguro a los datos y recursos del sistema o la red. Si se produce una infracción en la seguridad física, puede utilizarse un dispositivo como conexión de red remota que permita acceso sin restringir. Esto puede ocurrir sin conocimiento por parte del propietario del sistema o de los administradores de red.
Aunque los módems no se utilizan tanto como antes, muchos ordenadores todavía siguen incorporando módems internos. A menos que sean necesarios, deberían estar deshabilitados o eliminados en el terminal. Si no es posible, deberían estar configurados para que no respondan a las llamadas entrantes. En otras palabras, debe eliminar tantas características del módem como sea posible para incrementar la seguridad.
Muchos sistemas preconfigurados proporcionan conexiones de módem para el mantenimiento y el diagnóstico remoto. Estas deberían estar protegidas por una contraseña o contar con un conmutador de cierre para que la red no esté expuesta a infracciones de la seguridad.
<Nivel 2>Servicios de acceso remoto
<Cuerpo texto>El RAS (*Remote Access Services*, Servicios de acceso remoto) se refiere a cualquier servicio que ofrezca la posibilidad de conectar sistemas remotos. El producto actual de Microsoft para clientes basados en Windows se llama RRAS (*Routing and Remote Access Services*, Servicios de enrutamiento y acceso remoto) pero con anterioridad se conocían como RAS. Debido a ello, podrá observar que el término RAS se utiliza de forma indistinta para describir el producto de Microsoft y el proceso de conectarse a sistemas remotos. La figura 2.19 describe una conexión de marcado entre un terminal y una red empleando un servidor RAS. En este caso, la conexión se lleva a cabo entre un sistema basado en Windows y un servidor Windows que utiliza POTS (*Plain-Old Telephone Service*, Servicio telefónico antiguo/simple) y un módem.
**********2_019.tif**********
<Pie figura>**Figura 2.19.** Conexión RAS entre un terminal remoto y un servidor Windows.
<Cuerpo texto>La conexión RAS se consigue gracias a tecnologías de marcado o red como VPN, ISDN (*Integrated Services Digital Network*, Red digital de servicios integrados), DSL (***Digital Subscriber Line***, Línea de abonado digital) y módems de cable. Las conexiones RAS pueden ser seguras o estar fuera de peligro, dependiendo de los protocolos utilizados.
Un conocido de acceso remoto es el uso de PC Anywhere y programas similares de conexión de red remota/virtual. Una cuestión básica con VNC (*Virtual Network Computing*, Computación de red virtual) es que está dejando una puerta abierta en la red con la que cualquiera puede toparse. De forma predeterminada, la mayoría de programas inician el servicio del servidor automáticamente y este se ejecuta aunque no sea necesario. Por esta razón, se recomienda que configure el servicio para que se inicie de forma manual y solo se abra cuando sea necesario acceder al host. En las demás ocasiones, este servicio debería permanecer desactivado.
<Nivel 2>Enrutadores
<Cuerpo texto>El principal instrumento que se utiliza para la conectividad entre dos o más redes es el enrutador. Este dispositivo proporciona una ruta entre dichas redes. Para ello, utiliza dos conexiones. Cada una tiene su propia dirección y aparece como válida en su respectiva red. La figura 2.20 ilustra un enrutador conectado a dos redes LAN.
**********2_020.tif**********
<Pie figura>**Figura 2.20.** Enrutador conectado a dos redes LAN.
<Cuerpo texto>Los enrutadores son dispositivos inteligentes y, como tal, almacenan la información sobre las redes a las que están conectados. La mayoría de ellos pueden estar configurados para operar como cortafuegos de filtrado de paquetes. Los más novedosos también proporcionan funciones de cortafuegos avanzadas.
Los enrutadores, en combinación con CSU/DSU (*Channel Service Unit/Data Service Unit*, Unidad de servicio de canal/Unidad de servicio de datos), también se utilizan para traducir de un marco LAN (*Local Area Network*, Red de área local) a uno WAN (W*ide Area Network*, Red de área amplia) (por ejemplo, un enrutador que conecta una red 100BaseT a una T1). Se trata de algo necesario porque los protocolos de red son diferentes en LAN y WAN. Este tipo de dispositivos se conoce como enrutadores externos. Sirven como la conexión exterior de una LAN a una WAN y operan en el extremo de su red. Al igual que las patrullas fronterizas de muchos países, este tipo de enrutador decide quién puede entrar y bajo qué condiciones.
Dividir redes externas en dos o más suele ser habitual para los enrutadores. Además, pueden conectarse de forma interna a otros enrutadores, creando zonas que operen de forma autónoma. La figura 2.21 ilustra una red corporativa que utiliza la combinación de un enrutador externo para conectarse a un ISP (*Internet Service Provider*, Proveedor de servicios de Internet) y enrutadores internos para crear redes para la comunicación autónoma. Este tipo de conexión mantiene el tráfico de red local como la base de la red corporativa y proporciona una seguridad adicional a los usuarios internos.
**********2_021.tif**********
<Pie figura>**Figura 2.21.** Una red corporativa implementa enrutadores por cuestiones de segmentación y seguridad.
<Nota>**Truco:** Debido a que las difusiones no atraviesan los enrutadores, la segmentación de red reduce el tráfico.
<Cuerpo texto>Los enrutadores establecen la comunicación manteniendo tablas sobre destinos y conexiones locales. Un enrutador contiene información sobre los sistemas conectados a él y sobre el lugar al que envía solicitudes si el destino es desconocido. Estas tablas crecen según se van realizando conexiones a través del enrutador.
En general, estos dispositivos comunican el enrutamiento y otra información usando uno de los tres protocolos estándar. Este proceso puede tener lugar de forma interna o externa. A continuación, encontrará los tres protocolos a los que hacemos referencia:

<Sep-med>* **RIP (*Routing Information Protocol*, Protocolo de información de enrutamiento):** Protocolo simple que forma parte del entorno TCP/IP. Los enrutadores que utilizan RIP de forma rutinaria transmiten información sobre el estado y enrutamiento de los dispositivos conocidos. RIP también intenta encontrar rutas entre los dos sistemas usando el menor número de saltos o conexiones. Hay varias versiones de RIP disponibles, aunque la más utilizada hoy en día es la versión 2.
* **BGP (*Border Gateway Protocol*, Protocolo de puerta de enlace externa):** Este protocolo permite a grupos de enrutadores compartir información de enrutamiento.
* **OSPF (*Open Shortest Path First*, Abrir la ruta de acceso más corta primero):** Este protocolo permite que la información de enrutamiento se actualice con más rapidez que con RIP.
<Nota>**Nota:** En el mundo de Cisco, IGRP (*Interior Gateway Routing Protocol*, Protocolo de enrutamiento de puerta de enlace interior) y EIGRP (*Enhanced Interior Gateway Routing Protocol*, Protocolo de enrutamiento de puerta de enlace interior mejorado) se utilizan con frecuencia. Se trata de protocolos de distancia vectorial que calculan de forma matemática/automática las rutas y seleccionan la mejor.
<Cuerpo texto>Los enrutadores son su primera línea de defensa y deben estar configurados para que solo pueda pasar el tráfico autorizado por los administradores de red. En efecto, un enrutador puede funcionar como cortafuegos si se configura como tal. El mejor método es la superposición. Uno de estos dispositivos no debería ocupar el lugar de un cortafuegos pero sí aumentarlo.
Las rutas pueden configurarse como estáticas o dinámicas. Si son estáticas, se editan de forma automática y permanecen tal cual hasta que se modifican. Si son dinámicas, aprenden de otros enrutadores cercanos y utilizan esta información para crear sus tablas de enrutamiento.
<Nivel 2>Conmutadores
<Cuerpo texto>Los conmutadores son dispositivos que mejoran la eficacia de la red. En general, suelen tener una pequeña cantidad de información sobre los sistemas de una red. Utilizar conmutadores mejora la eficiencia de la red, en cuanto a los saltos, debido a la capacidad del circuito virtual. Estos dispositivos también mejoran la seguridad de la red porque examinar los circuitos virtuales es más difícil con los controladores de red. Puede pensar en los conmutadores como si se tratara de un dispositivo que tiene algunas de las mejores capacidades de los enrutadores y los concentradores juntos.
El conmutador mantiene información de enrutamiento limitada sobre los sistemas de la red interna y permite conexiones al igual que un concentrador. La figura 2.22 muestra un conmutador en acción entre dos terminales en una red LAN. La conexión no suele ser segura ni cifrada. No obstante, no deja el área conmutada y forma parte del tráfico de difusión general como suele ocurrir en una red LAN estrella o bus.
**********2_022.tif**********
<Pie figura>**Figura 2.22.** Conmutador entre dos sistemas.
<Nivel 2>Equilibradores de carga
<Cuerpo texto>Los equilibradores de carga se encargan del traslado de la carga de un dispositivo a otro. En la mayoría de ocasiones, el dispositivo en cuestión es un servidor, pero el término también podría emplearse para hacer referencia a un disco duro, una CPU o casi a cualquier dispositivo con el que quiera evitar la sobrecarga. Usando un servidor, equilibrar la carga entre varios servidores en lugar de depender solo de uno reduce el tiempo de respuesta, optimiza el rendimiento y permite la asignación de recursos.
Un equilibrador de carga puede instalarse como software o hardware y suele asociarse con un dispositivo, por ejemplo, un enrutador, un cortafuegos o un NAT. En la implementación más frecuente, el equilibrador de carga divide el tráfico de un sitio Web en solicitudes individuales que, con posteridad, rotan a servidores redundantes cuando éstos están disponibles (si un servidor que debería estar disponible está ocupado o bloqueado, no se tiene en cuenta para la rotación).
<Nivel 2>Sistemas Telecom/PBX
<Cuerpo texto>La capacidad de las telecomunicaciones ha experimentado cambios radicales en los últimos diez años. Los sistemas de telefonía y las tecnologías disponibles para abordar los temas de comunicación han proporcionado a muchas pequeñas empresas servicios de voz y datos integrados por completo a precios razonables.
Estos cambios han complicado la cuestión de la seguridad que debe implementarse. Una de las herramientas básicas en los sistemas de comunicación es PBX (*Private Branch Exchange*, Central de conmutación privada). Este sistema permite a los usuarios conectar voz, datos, localizadores, redes y casi cualquier aplicación concebible en un único sistema de telecomunicaciones. En resumen, un sistema PBX permite a una empresa ser su propia compañía telefónica.
La tecnología se está desarrollando hasta el punto de que todas las comunicaciones se producen a través de enlaces de datos para realizar llamadas telefónicas a las empresas usando tecnologías estándar de transmisión de datos, por ejemplo, T1 o T3. Esto significa que tanto las comunicaciones de voz como las de datos tienen lugar en la misma conexión de red para una compañía telefónica o un proveedor. Esto permite una única conexión para todas las comunicaciones para un único proveedor de estos servicios.
En principio, su sistema telefónico puede ser objeto de un ataque. La figura 2.23 muestra un sistema PBX conectado a una empresa telefónica usando una línea T1. En esta ilustración, la compañía telefónica se ha abreviado como OC (de Oficina Central). Los sistemas telefónicos de la empresa que gestionan el enrutamiento y la conmutación de llamadas y servicios se encuentran en la OC.
**********2_023.tif**********
<Pie figura>**Figura 2.23.** Sistema digital moderno PBX que integra voz y datos en una única conexión de red.
<Cuerpo texto>Si su sistema telefónico es parte de su red de comunicación de datos, un ataque podría acabar con él. Esto puede provocar que el nivel de estrés incremente de forma drástica en una ajetreada oficina.
**********INICIO DE NOTA**********

<Nivel 3>Encontrar los agujeros
<Nota>El Departamento de Comercio estadounidense, en combinación con el Instituto Nacional de Estándares y Tecnología, ha publicado un excelente artículo titulado "Análisis de la vulnerabilidad de PBX: Encontrar agujeros en su PBX antes de que alguien lo haga" *(PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does)* que encontrará en http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf. Este documento trata la arquitectura de sistema, el hardware, el mantenimiento y otras cuestiones relevantes para la administración diaria, así como para el examen.
**********FIN DE NOTA**********
<Cuerpo texto>En esta situación, también se incrementan los problemas de seguridad, ya que debe trabajar para salvaguardar las comunicaciones de voz. Cuando se redactaron las preguntas del examen, no había incidentes relacionados con sistemas telefónicos atacados por códigos maliciosos de los que tenga que estar al corriente. Desde entonces, se han comunicado algunos ataques de Voz sobre IP y puede que se conviertan en una gran preocupación en un futuro próximo.
**********INICIO DE NOTA**********
<Nota>**Truco:** Para el examen, debe saber que un PBX comparte muchas características con los demás componentes de red y que está sujeta a las mismas cuestiones, como dejar abiertos los puertos TCP. El PBX debería contar con auditorías y controles al igual que cualquier otro componente de red.
Imagine que alguien deja un mensaje de voz al presidente de su empresa. Un *phreaker* (alguien que abusa de los sistemas telefónicos, en contraposición a los sistemas de datos) puede interceptar este mensaje, alterarlo y devolverlo. El resultado de esta diablura podría convertirse en un poblema para la compañía (o al menos para el técnico de seguridad). No olvide cambiar la contraseña predeterminada en las cuentas de mantenimiento y en los sistemas para PBX tras su instalación, como haría con cualquier dispositivo de red.
**********FIN DE NOTA**********
<Nivel 2>Redes privadas virtuales
<Cuerpo texto>Una VPN es una conexión de red privada que se utiliza en una red pública. Este tipo de red proporciona seguridad frente a un entorno peligroso y, además, pueden emplearse para conectar redes LAN a través de Internet u otras redes públicas. En una VPN, el extremo remoto parece estar conectado a la red de forma local. Una red VPN requiere que se instale un hardware o un paquete de software VPN en los servidores y los terminales. En general, estas redes utilizan un protocolo de túnel, por ejemplo, L2TP , IPSec (*Internet Protocol Security*, Protocolo de seguridad de Internet)o PPTP (*Point-to-Point Tunneling Protocol*, Protocolo de túnel punto a punto). La figura 2.24 muestra una red remota conectada a una LAN usando Internet y una VPN. Parece una conexión local y todo el tráfico de mensajes y protocolos están disponibles a través de VPN.
**********2_024.tif**********
<Pie figura>**Figura 2.24.** Dos redes LAN conectadas usando VPN a través de Internet.
<Cuerpo texto>Las VPN se están convirtiendo en la conexión elegida cuando se establece una red externa o interna entre dos o más oficinas remotas. La principal preocupación en cuanto a seguridad es el cifrado. El protocolo PPTP ofrece algunas capacidades de cifrado aunque resultan algo débiles. IPSec proporciona mayor seguridad y está empezando a ser el sistema utilizado en muchos entornos VPN seguros.
<Nota>**Nota:** Aunque una red VPN se crea a través de Internet u otra red pública, la conexión formar parte de la red local de forma lógica. Esta es la razón por la que una conexión VPN utilizada para establecer una conexión entre dos redes privadas a través de Internet se considere una conexión privada o una red externa.
<Cuerpo texto>Como hemos mencionado en otras ocasiones, las redes VPN se emplean para establecer conexiones entre redes privadas a través de una red pública, como Internet. No se garantiza que sean seguras, a menos que utilice un protocolo de túnel (por ejemplo, PPTP) y un sistema de cifrado (como, IPSec). Tiene a su disposición una amplia variedad de opciones para VPN, incluyendo tecnologías de propiedad. Muchos de los grandes proveedores de ISP (*Internet Service Provider*, Proveedor de servicios de Internet) y datos ofrecen hardware especializados con capacidades VPN. Además, muchos servidores proporcionan opciones de software VPN.
Los sistemas VPN pueden estar dedicados a un protocolo en concreto o pasar cualquier protocolo que vean de un extremo de una red al otro. Una VPN pura aparece como una conexión de cable específica entre los extremos de dos redes.
Un concentrador VPN es un dispositivo de hardware utilizado para crear redes VPN de acceso remoto. Este crea unas sesiones cifradas de túnel entre host y suele emplear dos factores de autenticación para conseguir una seguridad adicional. Los modelos de Cisco es habitual que incorporen módulos SEP (*Scalable Encryption Processing*, Proceso de cifrado escalable) para permitir el cifrado basado en hardware y/o redundancia.
<Nivel 2>Puerta de enlace de seguridad Web
<Cuerpo texto>Una de los términos que más resuenan en estos momentos es la puerta de enlace de seguridad Web, un servidor proxy (que desempeña funciones de proxy y almacenamiento en caché) con un software de protección Web incorporado. Dependiendo del vendedor, la protección puede variar desde un escáner de virus estándar para paquetes entrantes hasta la comprobación del tráfico de salida de un usuario para marcarlo con banderas rojas.
Las posibles banderas rojas de la puerta de enlace pueden detectar/prohibir e incluir contenido inapropiado, intentando establecer una conexión punto a punto con un sitio de uso de archivos compartidos, mensajería instantánea y tunelado no autorizado. También tiene la capacidad de configurar la mayoría de las puertas de enlace de seguridad Web para bloquear explotaciones HTTP/HTML conocidas, etiquetas ActiveX, subprogramas Java y cookies.
<Nivel 2>Filtros de spam
<Cuerpo texto>Los filtros de spam pueden añadirse para filtrar correo electrónico no deseado antes de que se entregue de forma interna. El filtrado se realiza basándose en reglas establecidas (bloquear correos electrónicos entrantes procedentes de ciertas direcciones IP o correo electrónico con determinadas palabras en el asunto, por

mencionar algunas). Aunque estos filtros se suelen utilizar para escanear mensajes de entrada, también pueden emplearse para los mensajes de salida. De este modo, podría actuar como un identificador rápido de PC internos que puedan tener virus.
Se calcula que el 90 por ciento de los correos electrónicos que reciben muchas empresas son spam. SpamAssassin es uno de los filtros de acceso libre. Puede encontrar más información sobre él en http://spamassassin.apache.org/.
<Nota>**Nota:** Algunas empresas han creado dispositivos de seguridad "todo en uno" que combinan los filtros de spam con cortafuegos, equilibradores de carga y una serie de servicios adicionales.
<Nivel 1>Acceso remoto
<Cuerpo texto>Uno de los principales objetivos de tener una red es la posibilidad de conectar sistemas. Con el crecimiento de las redes, muchas tecnologías han aparecido para hacer que este proceso sea más fácil y más seguro. Un área clave de preocupación hace referencia a la conexión de sistemas y otras redes que no formen parte de su red. Las siguientes secciones describen los protocolos que se utilizan con más frecuencia para facilitar la conectividad entre sistemas remotos.
<Nota>**Nota:** Cualquier autenticación realizada por un usuario remoto se conoce como autenticación remota y suele llevarse a cabo usando TACACS (*Terminal Access Controller Access Control System* , Sistema de control de acceso mediante control del acceso desde terminales) o RADIUS (*Remote Authentication Dial In User Service*, Servicio de autenticación remota telefónica de usuario) (se tratarán más adelante).
<Nivel 2>Protocolo punto a punto
<Cuerpo texto>Presentado en 1994, PPP (*Point-to-Point Protocol*, Protocolo punto a punto) brinda soporte para múltiples protocolos entre los que se incluyen AppleTalk, IPX y DECnet. PPP funciona con POTS, ISDN y otras conexiones más rápidas como T1. PPP no proporciona seguridad de datos, pero ofrece autenticación usando el protocolo CHAP (*Challenge Handshake Authentication Protocol*, Protocolo de autenticación por desafío mutuo).
La figura 2.25 muestra una conexión PPP sobre una línea ISDN. En este caso, PPP suele utilizar un canal B de 64Kbps para la transmisión y permite que se conecten o asocien muchos canales para formar una única conexión virtual en una conexión de red.
**********2_025.tif**********
<Pie figura>**Figura 2.25.** PPP utilizando un único canal B en una conexión ISDN.
<Cuerpo texto>PPP funciona encapsulando el tráfico de red en un protocolo llamado NCP (*Network Control Protocol*, Protocolo de control de red). La autenticación la gestiona LCP (*Link Control Protocol*, Protocolo de control de enlace). Una conexión PPP permite a los usuarios remotos acceder a la red como si fueran usuarios locales. Sin embargo, no proporciona servicios de cifrado para el canal.
Como se habrá imaginado, la naturaleza insegura de PPP hace que no sea nada adecuada para conexiones WAN. Por esta razón, se han creado otros protocolos que sacan más partido a la flexibilidad de PPP y lo incorporan. Una conexión de marcado que utilice PPP funciona bien, ya que no es frecuente que un atacante pinche una línea telefónica. No obstante, debería confirmar que todas sus conexiones PPP utilizan canales seguros, conexiones específicas o de marcado.
Los usuarios remotos que se conecten directamente con un sistema utilizando conexiones de marcado no tienen por qué tener capacidades de cifrado habilitadas. Si la conexión es directa, la probabilidad de que alguien pudiera pinchar la línea telefónica existente es bastante reducida. Pero tendría que asegurarse de que las conexiones de la red usan un sistema de túnel orientado al cifrado.
<Nivel 2>Protocolos de túnel
<Cuerpo texto>Los protocolos de túnel añaden una capacidad a la red: la posibilidad de crear túneles entre redes que puedan ser más seguros, que presten soporte a protocolos adicionales y que proporcionen rutas virtuales entre los sistemas. La mejor forma de entender el tunelado es imaginar datos confidenciales encapsulados en otros paquetes que se envían a través de una red pública. Una vez que se reciben en el otro extremo, los datos confidenciales se extraen de los paquetes y se vuelven a compilar en su estado original
Los protocolos que se emplean con más frecuencia para el tunelado son los siguientes:
<Sep-med>* **PPTP:** Este protocolo presta soporte para la encapsulación en un único entorno punto a punto. PPTP encapsula y cifra los paquetes PPP. Esto lo convierte en el protocolo favorito de valor mínimo para las redes. La negociación de los extremos de una conexión PPTP se realiza fuera de peligro y, tras ella, se cifra el canal. Esta es una de las mayores debilidades de PPTP. Un dispositivo de captura de paquetes, por ejemplo, un analizador de protocolos sniffer, que detecta el proceso de negociación, podría utilizar esa información para determinar el tipo de conexión e información sobre el funcionamiento del túnel. Microsoft desarrolló PPTP y es compatible con la mayoría de productos de la empresa. PPTP usa el puerto 1723 y TCP para las conexiones.
* **L2F (Layer 2 Forwarding, Reenvío Capa 2):** Cisco creó este protocolo como un método de creación de túneles para conexiones de marcado. Es similar en capacidad a PPP y no se debería utilizar sobre redes WAN. Además, proporciona autenticación pero no cifrado. L2F usa el puerto 1701 y TCP para las conexiones.
* **L2TP:** No hace mucho tiempo, Microsoft y Cisco se pusieron de acuerdo para combinar sus respectivos protocolos en uno: L2TP. Este es un híbrido de PPTP y L2F. En esencia, se trata de un protocolo punto a punto. L2TP es compatible con numerosos protocolos de red y no solo puede utilizarse en redes TCP/IP, también funciona con IPX, SNA y IP, de modo que puede emplearse como puente en muchos tipos de sistema. El principal problema de L2TP es que no proporciona seguridad de datos: la información no está cifrada. La seguridad la ofrecen protocolos como IPSec. L2TP usa el puerto 1701 y UDP para las conexiones.
* **SSH (Secure Shell, Shell seguro):** Protocolo de túnel diseñado en su origen para sistemas Unix. Utiliza el cifrado para establecer una conexión segura entre dos sistemas. Además, proporciona programas alternativos que brindan seguridad para estándares Unix como Telnet, FTP y muchas otras aplicaciones orientadas a la comunicación. Hoy en día, SSH también está disponible para sistemas Windows. Esto lo convierte en el método de seguridad

favorito para Telnet y otros programas de escritura no cifrada en el entorno Unix. SSH usa el puerto 22 y TCP para las conexiones.

* **IPSec:** Este no es un protocolo de túnel pero se utiliza en combinación con este tipo de protocolos. Está orientado de forma básica hacia conexiones LAN, aunque también puede utilizarse con conexiones de marcado. IPSec proporciona una autentificación y un cifrado seguros de los datos y encabezados. Esto le convierte en una buena elección en términos de seguridad. IPSec puede funcionar en modo Túnel o Transporte. En modo Túnel, los datos o carga y los encabezados de mensaje están cifrados. En modo Transporte solo se cifra la carga.

**********INICIO DE NOTA**********

<Nivel 3>Conectar usuarios de redes remotas

<Nota>Su empresa quiere admitir conexiones de red para usuarios remotos. Éstos usarán Internet para acceder a sistemas de escritorio y otros recursos de la red. ¿Qué aconsejaría a la empresa?

Debería decir a su empresa que implemente un protocolo de túnel compatible seguro. Una buena solución sería una conexión VPN que utilice IPSec. También podría tener en cuenta protocolos como SSL, TLS y SSH como posibles opciones. Todos ellos ofrecen seguridad como parte de su proceso de conexión.

**********FIN DE NOTA**********

<Nivel 1>Resumen

<Cuerpo texto>En este capítulo hemos tratado los elementos clave de una infraestructura de red, como columna vertebral y clave de todas las medidas de seguridad que implemente en su red, y varios componentes relacionados con las conexiones..

La infraestructura incluye el hardware y el software necesarios para ejecutar su red. No olvide que los elementos esenciales para la seguridad son los enrutadores y los cortafuegos y que una configuración correcta es la clave para proporcionar servicios adaptados a las necesidades de su red. Si los dispositivos de seguridad de su red no están configurados de forma adecuada, puede tener consecuencias más graves que si no los tuviera. Si cree que está seguro pero, en realidad, no lo está, puede decirse que se encuentra en una situación peligrosa.

Las redes son cada vez más complicadas y están vinculadas a otras redes a una velocidad acelerada. Por este motivo, dispone de muchas herramientas que le ayudan a vincular y asegurar sus redes:

<Sep-med>* VPN.

* Protocolos de túnel.

* Acceso remoto.

<Cuerpo texto>Las conexiones que pueda realizar usando TCP/IP se basan, sobre todo, en direcciones IP. Cuando se asocian a un puerto estas direcciones, forman un punto final o *socket*. Este es el método más utilizado para comunicarse con servidores y aplicaciones como Web y Telnet. La mayoría de los servicios suelen tener *socket* estándar que operan de manera predeterminada, aunque puede intercambiarlos por configuraciones especiales y seguridad adicional. Cambiar los puertos predeterminados requiere que los usuarios sepan qué puertos proporcionan los servidores.

<Nivel 1>Ideas clave para el examen

<Cuerpo texto>A continuación, incluimos las ideas clave que debe recordar para el examen Security+:

<Sep-med>* **Descripción de varios componentes y el objetivo de una infraestructura:** La infraestructura de red es la columna vertebral de sus sistemas y operaciones de red. La infraestructura incluye todo el hardware, software, seguridad física y métodos operativos que ha implementado. Los componentes clave de su infraestructura incluyen dispositivos como enrutadores, cortafuegos, conmutadores, módems, sistemas de telecomunicaciones y otros dispositivos en la red.

* **Características de tecnologías de conectividad disponibles y capacidades de seguridad asociadas a cada una de ellas:** Acceso remoto, PPP, protocolos de túnel y VPN serán sus herramientas principales. PPTP y L2TP son dos de los protocolos utilizados con más frecuencia para el tunelado. IPSec, aunque no es un protocolo de túnel, proporciona un cifrado. Se suele emplear para mejorar la seguridad de túnel.

* **Manejo de las tecnologías utilizadas por TCP/IP e Internet:** Las direcciones IP y los números de puerto se combinan para crear una interfaz llamada punto final o *socket*. La mayoría de los protocolos TCP y UDP se comunican usando este *socket* como mecanismo principal de la interfaz. Los clientes y los servidores se comunican utilizando puertos. Éstos pueden modificarse para mejorar la seguridad. Por otro lado, los servicios Web utilizan HTML y otras tecnologías para permitir sitios Web enriquecidos y animados. Estas tecnologías pueden crear problemas de seguridad, ya que presentan vulnerabilidades individuales. Por ello, es aconsejable verificar los problemas que existen desde una perspectiva de seguridad antes de habilitar estas tecnologías en sus sistemas.

<Nivel 1>Prueba de evaluación

<Sep-med>1. ¿Cuál de los siguientes dispositivos es el más eficaz para proporcionar seguridad en la infraestructura?

A. Concentrador. **B.** Conmutador. **C.** Enrutador. **D.** Módem.

<Sep-med>2. Un superior ha determinado que debe colocarse un cortafuegos de forma inmediata, antes de que el sitio sufra un ataque similar al que ha destrozado una empresa del sector. Respondiendo a su petición, su jefe le explica que implemente un filtrado de paquetes para finales de semana. ¿Qué función realiza un filtrado de paquetes?

A. Evita que paquetes no autorizados entren en la red. **B.** Permite que todos los paquetes salgan de la red. **C.** Permite que todos los paquetes entren a la red. **D.** Elimina las colisiones en la red.

3. ¿Qué dispositivo almacena información sobre los destinos en una red?

A. Concentrador. **B.** Módem. **C.** Cortafuegos. **D.** Enrutador.

4. Cuando se han ido añadiendo más y más clientes a su red, la eficiencia de esta ha disminuido de forma considerable. Está preparando un presupuesto para el próximo año y quiere abordar este problema en particular. ¿Cuál de los siguientes dispositivos actúa como una herramienta para mejorar la eficiencia de la red?

A. Concentrador. **B.** Conmutador. **C.** Enrutador. **D.** PBX.
5. ¿Qué dispositivo se utiliza para conectar voz, datos, localizadores, redes y casi cualquier otra aplicación concebible en un único sistema de telecomunicaciones?
A. Enrutador. **B.** PBX. **C.** Concentrador. **D.** Servidor.
6. Se le ha comunicado a gran parte del personal de ventas que no informen a la oficina en una base diaria. A partir de ahora, tienen que pasar la mayoría del tiempo en la carretera llamando a los clientes. A cada miembro del personal de ventas se le ha proporcionado un ordenador portátil y se les ha pedido que se conecten a la red a través de una conexión de marcado cada noche. ¿Cuál de los siguientes protocolos se utiliza de forma generalizada hoy en día como protocolo de transporte para conexiones de marcado de Internet?
A. SMTP. **B.** PPP. **C.** PPTP. **D.** L2TP.
7. ¿Qué protocolo es inapropiado para conexiones VPN y WAN?
A. PPP. **B.** PPTP. **C.** L2TP. **D.** IPSec.
8. Le han dado la noticia de que pronto lo trasladarán a otro lugar. Antes de irse, tiene que realizar una auditoría en la red y justificar todo lo que utiliza y por qué lo utiliza. El próximo administrador empleará esta información para mantener la red en funcionamiento. ¿Cuál de los siguientes protocolos no es un protocolo de túnel pero es probable que los protocolos de tunelado lo utilicen por cuestiones de seguridad?
A. IPSec. **B.** PPTP. **C.** L2TP. **D.** L2F.
9. ¿Un *socket* es una combinación de qué componentes?
A. TCP y número de puerto. **B.** UDP y número de puerto. **C.** IP y número de sesión. **D.** IP y número de puerto.
10. Está explicando los protocolos a un administrador novel poco antes de irse de vacaciones. Surge el tema de las aplicaciones de correo electrónico de Internet y le explica cómo se han realizado las conexiones y cómo espera que se realicen en el futuro. ¿Cuál de los siguientes protocolos se está convirtiendo en el estándar más novedoso para las aplicaciones de correo electrónico de Internet?
A. SMTP. **B.** POP. **C.** IMAP. **D.** IGMP.
11. ¿Qué protocolo se suele utilizar para la información de mantenimiento y destino?
A. ICMP. **B.** SMTP. **C.** IGMP. **D.** Enrutadores.
12. Es el administrador de Mercury Technical. Gracias a una comprobación de los protocolos en uso de su servidor descubre que había uno en uso y no era consciente de ello. Sospecha que alguien lo está utilizando para enviar mensajes a varios receptores. ¿Cuál de los siguientes protocolos se utiliza para enviar mensajes de grupo o mensajería multidifusión?
A. SMTP. **B.** SNMP. **C.** IGMP. **D.** L2TP.
13. IPv6, además de tener más bits asignados para cada dirección host, ¿para qué protocolo de seguridad tiene también requisitos obligatorios?
A. TFPT. **B.** IPSec. **C.** SFTP. **D.** L2TP.
14. ¿Qué puertos está reservados de forma predeterminada para que lo utilice FTP? (Hay varias opciones correctas.)
A. 20 y 21 TCP. **B.** 20 y 21 UDP. **C.** 22 y 23 TCP. **D.** 22 y 23 UDP.
15. ¿Cuál de los siguientes servicios solo se utiliza en puertos TCP y no UDP? (Hay varias opciones correctas.)
A. IMAP. **B.** LDAP. **C.** FTPS. **D.** SFTP.
16. ¿Cuál de las siguientes puede implementarse como una solución de software o hardware y se suele asociar con un dispositivo, por ejemplo, un enrutador, un cortafuegos o NAT, y se utiliza para trasladar carga de un dispositivo a otro?
A. Proxy. **B.** Concentrador. **C.** Equilibrador de carga. **D.** Conmutador.
17. ¿Cuáles de los siguientes son dispositivos con varios puertos que mejoran la eficacia de la red?
A. Conmutadores. **B.** Módems. **C.** Puertas de enlace. **D.** Concentradores.
18. ¿Qué servicio/-s utilizan de forma predeterminada el Puerto 22 TCP y UDP? (Hay varias opciones correctas)
A. SMTP. **B.** SSH. **C.** SCP. **D.** IMAP.
19. ¿Qué protocolo, ejecutado sobre TCP/IP, se suele utilizar para el registro y la resolución de nombres con clientes basados en Windows?
A. Telnet. **B.** SSL. **C.** NetBIOS. **D.** TLS.
20. ¿Cuántos bits se utilizan para el direccionamiento con IPv4 e IPv6?
A. 32,128. **B.** 16,64. **C.** 8,32. **D.** 3,16.
<Nivel 1>Respuestas de la prueba de evaluación
<Sep-med>1. C. Los enrutadores pueden configurarse en muchos casos para actuar como cortafuegos de filtrado de paquetes. Si los configura de forma adecuada, pueden evitar que se abran puertos no autorizados.
2. A. El filtrado de paquetes evita que paquetes no autorizados abandonen o entren en la red. Este filtrado es un tipo de cortafuegos que bloquea el tráfico de puertos específicos.
3. D. Los enrutadores almacenan información sobre los destinos de red en las tablas de enrutamiento. Estas contienen información sobre los host en ambos lados del enrutador.
4. B. Los conmutadores crean circuitos virtuales entre sistemas en una red. Estos circuitos son privados y reducen el tráfico de red cuando se utilizan.
5. B. Muchos sistemas PBX modernos integran voz y datos en una única conexión de datos con el proveedor de su servicio telefónico. En algunos casos, esto permite un coste general del coste de las operaciones. Estos enlaces se realizan utilizando conexiones de red existentes como T1 o T3.
6. B. PPP puede pasar múltiples protocolos y se usa como protocolo de transporte para conexiones de marcado.

7. A. PPP no proporciona seguridad y todas las actividades son inseguras. PPP está ideado para conexiones de marcado y nunca debería emplearse en conexiones VPN.
8. A. IPSec proporciona seguridad de red para protocolos de túnel. Puede utilizarse con muchos protocolos diferentes además de TCP/IP y tiene dos modos de seguridad.
9. D. Un *socket* es una combinación de direcciones IP y números de puerto. El *socket* identifica qué aplicación responderá a la solicitud de red.
10. C. IMAP se está convirtiendo en el estándar más popular para los clientes de correo electrónico y está sustituyendo a protocolos POP para sistemas de correo electrónico. Además, permite que el correo se reenvíe y se acumule en áreas de información llamadas almacenes.
11. A. IGMP se usa para funciones de destino y error en TCP/IP. Es enrutable y lo emplean programas como Ping y Traceroute.
12. C. IGMP se utiliza para mensajería en grupo y multidifusión. Mantiene una lista de sistemas que pertenecen a un grupo de mensajes. Cuando se envía un mensaje a un grupo en concreto, cada sistema recibe una copia individual.
13. B. La implementación de IPSec es obligatoria con IPv6. Aunque se suele hacer con IPv4, no es un requisito.
14. A. FTP utiliza los puertos TCP 20 y 21. FTP no utiliza puertos UDP.
15. D. SFTP solo utiliza puertos TCP. IMAP, LDAP y FTPS utilizan puertos TCP y UDP.
16. C. Un equilibrador de carga puede implementarse como solución de software o hardware y se suele asociar con un enrutador, un cortafuegos o NAT. Como su nombre indica, se utiliza para trasladar carga de un dispositivo a otro.
17. A. Los conmutadores son dispositivos con varios puertos que mejoran la eficiencia de la red. En general, tiene una pequeña cantidad de información sobre los sistemas de una red.
18. B, C. El puerto 22 lo utilizan SSH y SCP con TCP y UDP.
19. C. NetBIOS se emplea para el registro y la resolución de nombres con clientes basados en Windows. Se ejecuta sobre TCP/IP.
20. A. IPv4 utiliza 32 bits para la dirección de host, mientras que IPv6 usa 128 bits para ello.

Capítulo 3. Proteger redes

<Cuerpo texto>En este capítulo se tratan los siguientes objetivos del examen CompTIA Security+:
<Sep-med>3.1 Analizar y diferenciar los distintos tipos de software malintencionado.
3.5 Analizar y diferenciar los tipos de ataques de aplicación.
3.6 Analizar y diferenciar las distintas técnicas de mitigación y disuasión.
3.7 Implementar herramientas y técnicas de evaluación para descubrir las amenazas y debilidades de la seguridad.
4.1 Explicar la importancia de la seguridad de uso.
<Cuerpo texto>El primer capítulo se centraba en las distintas formas de riesgo y cómo calcularlas, mientras que el segundo describió la tecnología sobre la que se construye la red y algunos de los dispositivos que pueden mitigar parte del riesgo. Este capítulo se centrará en la identificación de problemas relacionados con la seguridad cuando estos se producen;
en detectar y prevenir la intrusión si la red es básica o local; en proporcionar métodos clave para identificar intrusos, y en la información que se debe dar a los administradores cuando necesiten respuestas. Además de estos controles, puede crear trampas para aquellos que violen la seguridad, como *honeypots* y *honeynets* que atraen a los intrusos y le permiten seguirles la pista o atraparlos.
Por último, este capítulo se aborda algunos conceptos clave de la seguridad de uso y problemas de los que debería ser consciente.
<Nivel 1>Controlar y diagnosticar las redes
<Cuerpo texto>Es importante controlar la red y asegurarse de que el tráfico que hay en ella es el que corresponde. En esta sección, analizaremos los controles de red básicos, así como sistemas para detectar la intrusión.
<Nivel 2>Monitor de red
<Cuerpo texto>Los monitores de red, también conocidos como *sniffers*, se crearon, en principio, para facilitar la resolución de problemas de red. Los programas de configuración de red simples, como Ipconfig, no entran en el cableado y no comunican lo que está ocurriendo en la parte física de una red. Por lo quepara analizar la señalización y el tráfico que se produce en una red se necesita un monitor de red. Los primeros monitores eran voluminosos y su uso requería un alto nivel de especialización. Como suele pasar con casi todo en la era informática, ahora son más simples, pequeños y económicos. Por otro lado, los controles de red están disponibles para la mayoría de entornos y son muy efectivos y fáciles de usar.
Hoy en día, un sistema de monitorización de red suele consistir en un PC con una NIC (en modo promiscuo) y un software de monitorización. Este es un menú de control fácil de utilizar y tiene un archivo de ayuda muy completo. El tráfico que visualizan los *sniffers* puede ser demasiado complejo y requerir materiales técnicos adicionales quepodrá comprar en la mayoría de librerías o encontrarlos en Internet de forma gratuita. Con unas pocas horas de trabajo, se puede conseguir que los monitores de red funcionen con eficacia y usen los datos que presentan.
<Nota>**Truco:** Los productos de Windows Server incluyen un servicio llamado Network Monitor que puede descargar para obtener información básica sobre el tráfico de red. En SMS (*Systems Management Server*, Servidor de gestión de sistemas) se incluye una versión más completa y detallada de Network Monitor. En lo que se refiere a productos de terceros, Wireshark, disponible para la mayoría de plataformas, es líder en el mercado (para más información, véase http://www.wireshark.org/).
<Nota>**Nota:** Sniffer es un nombre comercial, como Kleenex. Es el hardware de monitor de red más conocido, por eso, todo el mundo empezó a llamarlos *sniffers*.
<Nivel 2>Sistemas de detección de intrusos
<Cuerpo texto>Un IDS (*Intrusion Detection System*, Sistema de detección de intrusiones) es un software que se ejecuta en terminales individuales o dispositivos de red con el fin de monitorizar y registrar la actividad de red. Usando un IDS, un administrador puede configurar el sistema para responder igual que una alarma de robo. Los IDS pueden prepararse para evaluar sistemas de acceso, centrarse en actividades de red sospechosas y desconectar sesiones que no cumplan los requisitos de seguridad.
Muchos proveedores han hecho una propaganda excesiva de la simplicidad de estos sistemas. Sin embargo, son bastante complejos y requieren un alto grado de planificación y mantenimiento para que funcionen de forma efectiva. Por otro lado, muchos fabricantes están vendiendo IDS con cortafuegos,lo cual es una idea que promete. Por sí mismos, los cortafuegos evitarán muchos ataques comunes, pero no suelen tener ni inteligencia ni capacidades de notificación para monitorizar toda la red. Un IDS, en combinación con un cortafuegos, permite una actitud reactiva, debido al cortafuegos y una preventiva, gracias al IDS.
La figura 3.1 ilustra un IDS trabajando en combinación con un cortafuegos para incrementar la seguridad.
**********3_001.tif**********
<Pie figura>**Figura 3.1.** Un IDS trabajando con un cortafuegos para incrementar la seguridad.
<Cuerpo texto>Si el cortafuegos pierde su confidencialidad o se produce una invasión, el IDS puede reaccionar deshabilitando sistemas, terminando sesiones e incluso desconectando la red. Esta estructura proporciona mayor nivel de seguridad que estos dos dispositivos de forma aislada. Trataremos con más detalle los IDS en la siguiente sección.
<Nivel 1>El sistema de detección de intrusiones
<Cuerpo texto>En las películas originales de *Pisando fuerte* (*Walking Tall*), el *sheriff* colocaba pequeñas tiras de cinta adhesiva transparente en el capó de su coche. Antes de entrar en el vehículo, comprobaba si la cinta, muy difícil de detectar, estaba rota. Esto le advertía si alguien había estado husmeando bajo el capó. Eso, en ocasiones, le salvaba la vida. ¿Tiene cinta adhesiva en su red?

Los IDS se están convirtiendo en partes integrales de la monitorización de red. Se trata de una tecnología algo reciente y promete mucho en la detección de intrusiones de red. El ID (*Intrusion Detection*, Detección de intrusiones) es el proceso de monitorizar eventos en un sistema o red para determinar si se ha producido una intrusión. Este término se define como toda actividad o acción que intenta minar o comprometer la confidencialidad, integridad o disponibilidad de los recursos. Como recordará, los cortafuegos están diseñados para evitar que un atacante acceda a los recursos. Un IDS informa y monitoriza los intentos de intrusión.
**********INICIO DE NOTA**********
<Nivel 3>Conocer los recursos disponibles en Linux
<Nota>Hay información sobre seguridad disponible en numerosos sitios relacionados con Linux. Lo primero que debería comprobar siempre es el sitio del distribuidor. Sus páginas suelen proporcionar una perspectiva general sobre cuestiones de seguridad con enlaces a otras páginas relevantes. También debería estar al tanto de los temas y problemas que se publiquen en http://www.cert.org y http://www.linuxsecurity.com.
Además, puede encontrar información a través de los comandos de Linux gracias a una variedad de utilidades inherentes que este posee:
<Sep-med>* La herramienta man ofrece páginas sobre cada utilidad. Por ejemplo, para encontrar información relacionada con la herramienta setfacl, puede escribir **man setfacl**.
* La mayoría de utilidades tienen la opción -help incorporada para ofrecer información. Desde la línea de comando, puede escribir **setfacl -help** para acceder a una lista con las opciones disponibles.
* La utilidad info también visualiza las páginas man.
* La utilidad whatis puede mostrar si hay más de un paquete de documentación en el sistema.
* La utilidad whereis enumera toda la información que puede encontrar sobre localizaciones asociadas con un archivo.
* La utilidad apropos usa la base de datos whatis para encontrar valores y devolver un breve resumen de la información.
**********FIN DE NOTA**********
<Nota>**Nota:** Se entiende de forma implícita que todas las redes, sin tener en cuenta el tamaño, deberían utilizar un cortafuegos. En una red doméstica, se puede implementar un software personal para proporcionar protección frente a los ataques.
<Cuerpo texto>Hay muchos términos necesarios para explicar la tecnología que hay detrás de la detección de intrusiones. Entre ellos, los siguientes:
<Sep-med>* **Actividad:** Elemento de una fuente de datos que resulta de interés para el operador. Podría incluir una incidencia específica del tipo de actividad sospechosa. Un ejemplo podría ser la solicitud de una conexión TCP producida en repetidas ocasiones desde de la misma dirección IP.
* **Administrador:** Persona responsable de establecer la política de seguridad de una empresa y de tomar decisiones sobre la implementación y la configuración del IDS. El administrador debería adoptar ciertas actitudes con respecto a los niveles de alarma, el registro histórico y las capacidades de monitorización de las sesiones. También es responsable de determinar respuestas apropiadas a ataques y asegurar que estas se llevan a cabo.
<Nota>**Truco:** La mayoría de las empresas tienen un diagrama jerárquico. Es raro que el administrador esté en lo alto del diagrama, pero siempre se espera que haga todo lo posible por mantener los incidentes bajo control.
<Sep-med>* **Alerta:** Mensaje procedente del analizador que indica que se ha producido un evento de interés. La alerta contiene información sobre la actividad, así como especificaciones de la incidencia. Puede que se genere una alerta si se produce un tráfico de ICMP (o si están fallando intentos de acceso repetidos. Es normal que haya un cierto nivel de tráfico en una red. Las alertas tienen lugar cuando las actividades de un determinado tipo exceden el umbral preestablecido. Por ejemplo, puede que quiera generar una alerta cada vez que alguien del exterior utilice el programa Ping para enviar *pings*.
* **Analizador:** Componente o proceso que estudia y busca actividad sospechosa entre los datos recopilados por el sensor. Los analizadores funcionan monitorizando eventos y determinando si producen movimientos inusuales. También pueden utilizar un proceso basado en las reglas establecidas al configurar el IDS.
* **Fuente de datos:** Información sin pulir que usa el IDS para detectar actividad sospechosa. La fuente de datos puede incluir archivos de auditorías, accesos de sistema o tráfico de red.
* **Evento:** Incidencia que tiene lugar en una fuente de datos que indica que se ha producido una actividad sospechosa. Normalmente se envía una notificación comunicando que puede estar ocurriendo algo inusual en la red. Un IDS también puede iniciar eventos de acceso si el volumen de conexiones de correo electrónico entrantes se detiene de repente, lo cual puede ser indicio de que alguien está sondeando su red. Es posible que este evento desencadene una alerta si se produce una desviación de los patrones del tráfico de red habitual o si alguna actividad sobrepasa el umbral.
* **Supervisión:** Componente o proceso que usa el operador para gestionar el IDS. La consola IDS es un único supervisor, cuyos cambios de configuración se realizan comunicándose con el supervisor del IDS.
* **Notificación:** Proceso o método por el que el supervisor del IDS comunica una alerta al operador. Podría incluir un gráfico destacando el tráfico o el envío de un correo electrónico al personal de administración de la red.
* **Operador:** Persona que está a cargo del IDS. Puede ser un usuario o un administrador y, por supuesto, siempr que sean responsables directos.
* **Sensor:** Componente del IDS que recopila información de la fuente de datos y la pasa al analizador. Un sensor puede ser un controlador de dispositivo en un sistema o una caja negra conectada a la red que informa al IDS. Lo importante es recordar que es el principal punto de recopilación de datos para el IDS.
<Cuerpo texto>Como puede observar, el IDS tiene muchos componentes y procesos diferentes que trabajan juntos para ofrecer una panorámica en tiempo real del tráfico de red. Compruebe en la figura 3.2 los componentes y

procesos que funcionan de forma conjunta para proporcionar un IDS. Recuerde que los datos pueden proceder de distintas fuentes y deben analizarse para determinar qué está ocurriendo. Un IDS no es un auténtico dispositivo para bloquear el tráfico, aunque algunos incluyan esta función. Sobre todo se pretende que sea un dispositivo para realizar auditorías en los datos.

**********3_002.tif**********

<Pie figura>**Figura 3.2.** Componentes de un IDS trabajando juntos para monitorizar la red.

<Cuerpo texto>Los IDS emplean, fundamentalamente, cuatro enfoques :

<Sep-med>* **Detección IDS basada en el comportamiento:** Sistema basado en el comportamiento que busca variaciones de naturaleza conductual, como un tráfico más elevado de lo habitual o la violación de políticas, entre otros. Al buscar desviaciones de comportamiento se pueden reconocer hipotéticas amenazas y responder a ellas con rapidez.

* **Detección IDS basada en la firma:** Sistema basado en la firma, también conocido como MD-IDS (*Misuse-Detection IDS*, Detección IDS de uso incorrecto), que se centra, sobre todo, en evaluar ataques basándose en rastros de firma y auditorías. Los ataques de firma describen un método establecido, en general, para atacar un sistema. Por ejemplo, un ataque de desbordamiento TCP se inicia con un gran número de sesiones TCP incompletas. Si el MD-IDS sabe detectar este tipo de ataque, puede realizar un informe adecuado o responder para desbaratar dicho ataque. La figura 3.3 ilustra un IDS, basado en la firma, en acción. Observe que este IDS usa una base de datos extensa para determinar la firma del tráfico. Este proceso recuerda al de un software antivirus.

**********3_003.tif**********

<Pie figura>**Figura 3.3.** IDS, basado en la firma, en acción.

<Sep-med>* **Detección IDS de anomalías:** Un AD-IDS (*Anomaly-detection IDS*, IDS de detección de anomalías) busca anomalías, es decir, elementos fuera de lo común. En general, un programa normal de formación enseña cuál es la operación normal y, con posterioridad, extrae las desviaciones de esta. Un AD-IDS establece la línea de base con los valores asignados de forma manual o a través de un proceso automatizado que se centra en patrones de tráfico. Uno de los métodos está basado en el comportamiento, el cual busca conductas inusuales y actúa en consecuencia.

* **IDS heurístico:** Este tipo de sistema utiliza algoritmos para analizar el tráfico que pasa a través de la red. Como regla general, los sistemas heurísticos requieren más ajustes y precisión que otros sistemas de detección que evitan falsos positivos en su red.

<Cuerpo texto>Los IDS se centran en informar de eventos o tráfico de red que se desvíe de la actividad de trabajo histórica o de los patrones del tráfico de red. Para que este informe sea efectico, los administradores deberían desarrollar una línea de base o un historial del tráfico de red habitual. Esta línea proporciona una perspectiva estable y a largo plazo de la actividad de una red. Un ejemplo podría ser un informe generado cuando se reciba un nivel de respuestas ICMP superior al habitual en un período de tiempo específico. Esta actividad indicaría el comienzo de un ataque de desbordamiento ICMP. El sistema también informaría del momento en que un usuario poco frecuente accede a la red usando VPN y solicite de repente acceso administrativo al sistema. La figura 3.4 muestra un AD-IDS que registra e informa de un tráfico excesivo en una red. El proceso AD-IDS suele utilizar inteligencia artificial o tecnologías de sistema expertas para aprender cuál es el tráfico normal en una red.

**********3_004.tif**********

<Pie figura>**Figura 3.4.** Un AD-IDS utilizando tecnologías de sistema expertas para evaluar riesgos.

<Nota>**Truco:** Siempre que se produce un ataque, suele ocurrir algo que lo delata: una entrada en el registro de acceso, un error de acceso, por mencionar algunos ejemplos. Estos elementos representan firmas de intrusión. Puede identificarlos e instruir un IDS para que busque y evite nuevas actuaciones de estos elementos.

<Cuerpo texto>MD-IDS (*Misuse-Detection IDS*, Detección IDS de uso incorrecto) y AD-IDS se combina en la mayoría de sistemas comerciales, proporcionando una oportunidad única para detectar y desbaratar ataques y accesos no autorizado. Al contrario que un cortafuegos, el objetivo del IDS es detectar e informar de incidencias inusuales en una red, pero no bloquearlas.

Los siguientes apartados hablan sobre las implementaciones basadas en red y en host de IDS, así como las capacidades que proporcionan. También se describe el término *honeypots* o respuesta a incidencias.

<Nivel 2>Trabajar un IDS basado en red

<Cuerpo texto>Un enfoque NIDS (*Network-Based IDS*, Sistema de detección de intrusión basado en red) para IDS proporciona al sistema un punto en la red que puede monitorizar e informar de todo el tráfico de red. Este puede estar delante o detrás del cortafuegos, como puede observar en la figura 3.5.

**********3_005.tif**********

<Pie figura>**Figura 3.5.** Colocar NIDS en una red determina qué datos se analizarán.

<Nota>**Nota:** La mejor solución para crear una red segura es colocar IDS delante y detrás del cortafuegos. Esta doble seguridad proporciona la mayor defensa posible.

<Cuerpo texto>Colocar el NIDS delante del cortafuegos proporciona la monitorización de todo el tráfico de red entrante. Este enfoque le permite procesar una enorme cantidad de datos, además de ver todo el tráfico que entra en la red. Colocar el NIDS detrás del cortafuegos le permite ver únicamente el tráfico que consigue superar la barrera de seguridad del cortafuegos. Aunque el NIDS reduce la cantidad de datos procesados, no le permite ver todos los ataques que se puedan estar desarrollando.

El NIDS puede adjuntarse a un conmutador o concentrador, así como a una llave. Muchos concentradores y conmutadores proporcionan un puerto de monitorización por cuestiones de resolución de problemas y diagnóstico. Este puerto puede funcionar de modo similar a una llave. La ventaja de este enfoque es que el IDS es el único dispositivo que usará la llave. La figura 3.6 ilustra la conexión de una red usando un concentrador o llave.

**********3_006.tif**********

<Pie figura>**Figura 3.6.** Se utiliza un concentrador para adjuntar el NIDS a la red.
<Nota>**Nota:** La expansión de puerto, también conocida como creación de reflejo de puerto, copia el tráfico de todos los puertos en un único puerto y deshabilita el tráfico bidireccional en él. El SPAN (*Switched Port Analyzer*, Analizador de puertos conmutados) de Cisco es un ejemplo de implementación de la expansión de puerto.
<Cuerpo texto>En cualquier caso, el IDS monitoriza y evalúa todo el tráfico al que tiene acceso.
A nivel de red, se pueden formular dos tipos de respuesta básicas: pasiva y activa. Ambas se explican de forma breve en los siguientes apartados.
**********INICIO DE NOTA**********
<Nivel 3>Trabajar con archivos de auditoría de red
<Nota>Imagine que es el administrador de una red bastante transitada. La empresa ha sufrido un par de recortes y el personal es limitado. Quiere tener la certeza de que su red sigue siendo tan segura como le sea posible. ¿Qué puede hacer para aminorar el volumen de trabajo?
Tiene tres posibilidades. Hay dos que debería tener en cuenta para proteger su red: instalar un IDS o reducir los niveles de acceso a los archivos de auditorías en red. Para ellopuede utilizar un sistema de recopilación de registros de auditorías.
También tiene la posibilidad de reducir la cantidad de tráfico registrado en sus archivos de auditoría cambiando la configuración que determina qué auditar. Sin embargo, modificar las reglas de autorías evitaría que viera lo que está ocurriendo en su red debido a que no quedarían grabados la mayoría de registros.
Instalar un IDS le permitirá establecer normas que proporcionen un nivel de automatización que revise los archivos de auditoría. Puede que la solución más adecuada sea convencer a su empresa para invertir en un IDS, ya que podría enviar un correo electrónico o una alerta cuando se detectara un evento.
**********FIN DE NOTA**********
<Nivel 3>Implementar una respuesta pasiva
<Cuerpo texto>La respuesta pasiva es la más común para muchas intrusiones. En general, suele ser la más fácil de desarrollar e implementar. La siguiente lista incluye algunas estrategias de respuesta pasiva:
<Sep-med>* **Registro:** Anota que se ha producido un evento y bajo qué circunstancias ha tenido lugar. Las funciones de registro deberían proporcionar suficiente información sobre la naturaleza del ataque para ayudar a los administradores a determinar qué ha sucedido y asistirles cuando evalúen la amenaza. Con posterioridad, esta información puede utilizarse para idear métodos que contengan el peligro.
* **Notificación:** Comunica la información relacionada con un evento al personal adecuado, en caso de que se produzca. Esto incluye transmitir cualquier dato relevante sobre el evento que ayuda a evaluar la situación. Si el IDS se controla todo el tiempo, los mensajes pueden visualizarse en la consola del supervisor para indicar qué situación se está produciendo.
* **Elusión:** Evitar o ignorar un ataque suele ser una respuesta habitual. Este puede ser el caso si su IDS observa que se está iniciando un ataque IIS (*Internet Information Server*, Servidor de información de Internet) en un sistema que está ejecutando otro servicio hospedado en Web, como Apache. El ataque no funcionaría porque Apache no responde del mismo modo que IIS. ¿Qué sentido tiene entonces prestarle atención a este problema? En una red muy transitada, se pueden producir diferentes ataques a la vez. Si no le preocupa que tenga lugar un ataque, ¿por qué malgastar su tiempo y energía investigando sobre ello o notificándolo a alguien más? El IDS puede tomar nota en un registro y pasar a otro asunto más prioritario.
<Nota>**Truco:** Recuerde que las respuestas pasivas son las que se implementan con más frecuencia, ya que son las menos costosas y las más fáciles de poner en práctica.
<Nivel 3>Implementar una respuesta activa
<Cuerpo texto>Una respuesta activa implica ejecutar una acción a partir de un ataque o amenaza. El objetivo de este tipo de respuesta es llevar a cabo una acción lo antes posible para reducir el impacto del evento.
Esta acción requiere planificar y gestionar un evento, políticas claras e inteligencia en el IDS para alcanzar el éxito. Una respuesta activa incluirá una de las reacciones descritas con brevedad a continuación:
<Sep-med>* **Poner fin al proceso o sesión:** Si se detecta un ataque de desbordamiento, el IDS puede provocar que el subsistema, como TCP, se vea forzado a reiniciar todas las sesiones que están en marcha. Con ello, libera los recursos y permite que TCP siga operando con normalidad. Por supuesto, todas las sesiones TCP válidas se cerrarán y tendrán que restablecerse, aunque esto puede tener pequeños efectos en los usuarios finales. El IDS evalúa los eventos y determina el mejor modo de gestionarlos. La figura 3.7 ilustra TCP redirigiéndose para emitir comandos RST desde el IDS y restablecer todas las conexiones abiertas a TCP. Este tipo de mecanismo también puede terminar sesiones de usuario o detener y reiniciar cualquier proceso que parezca estar operando de forma poco habitual.
**********3_007.tif**********
<Pie figura>**Figura 3.7.** IDS comunicando a TCP que restablezca todas las conexiones.
<Sep-med>* **Cambios en la configuración de red:** Si se descubre que una dirección IP determinada está provocando repetidos ataques en la red, el IDS puede comunicar a un enrutador fronterizo o a un cortafuegos que rechace cualquier petición o tráfico procedente de la dirección en cuestión. Este cambio en la configuración puede estar vigente de forma continuada o durante un período específico. La figura 3.8 ilustra el IDS comunicando al cortafuegos que cierre el puerto 80 durante 60 segundos para detener un ataque IIS. Si el IDS determina que está siendo atacado un *socket* o puerto en particular, puede comunicar al cortafuegos que lo bloquee durante un período de tiempo concreto. Con ello, elimina de forma efectiva el ataque pero también puede provocar, sin darse cuenta, una situación DoS que suprima el tráfico ilegítimo, sobre todo, en el caso del puerto 80 (HTTP o Web).
**********3_008.tif**********
<Pie figura>**Figura 3.8.** IDS comunicando al cortafuegos que cierre el puerto 80 durante 60 segundos para desbaratar un ataque IIS.

<Sep-med>* **Engaño:** Esta respuesta activa hace pensar al agresor que el ataque se está produciendo mientras que, en realidad, el sistema monitoriza la actividad y lo redirige a otro sistema que ha sido ideado para destruirlo. Este sistema permite al operador recopilar datos sobre cómo se lleva a cabo el ataque y qué técnicas se están utilizando. Si lo traducimos al español, este proceso se conoce como "enviarlos al tarro de miel o *honeypot*" y se describe más adelante. La figura 3.9 ilustra un *honeypot* en el que el engaño resulta todo un éxito.
**********3_009.tif**********
<Pie figura>**Figura 3.9.** Un honeypot desvía a un atacante y acumula inteligencia.
<Sep-med>La ventaja de este tipo de respuesta es que se contemplan y registran todas las actividades para el análisis cuando el ataque ha concluido. Se trata de un escenario difícil de configurar ya que es peligroso permitir a un *hacker* avanzar en su red, con independencia de que esté monitorizando los eventos o no.
Este enfoque se suele utilizar cuando las fuerzas del orden público están llevando a cabo una investigación y están recopilando pruebas para asegurar el éxito de la acusación al atacante. El engaño le permite recabar documentación sin poner en riesgo sus datos.
<Nota>**Truco:** Recuerde que las respuestas activas son las que se realizan con menos frecuencia. Las más efectivas son las más costosas y las más complicadas de poner en práctica, por no mencionar el problema en el que puede verse si sigue la estrategia de atacar a los que nos atacan.
<Nivel 2>Trabajar con un Sistema de Detección de Intrusión Basado en Host
<Cuerpo texto>Un HIDS (*Host-Based IDS*, Sistema de detección de intrusión basado en host) está diseñado para ejecutar un software en un sistema informático host. En general, este tipo de sistemas funciona como un servicio o un proceso de fondo. Los HIDS analizan los registros de la máquina, los eventos del sistema y las interacciones de las aplicaciones, pero no suelen monitorizar el tráfico de red que entra al host. Son habituales en servidores que utilizan canales de cifrado o para otros servidores.
La figura 3.10 ilustra un IDS instalado en un servidor. Observe que el HIDS interactúa con los archivos de las auditorías de inicios de sesión y con los del núcleo. Estos últimos se utilizan para interfaces de proceso y aplicación.
**********3_010.tif**********
<Pie figura>**Figura 3.10.** Un IDS basado en host que interactúa con el sistema operativo.
<Cuerpo texto>Dos de los principales problemas que presenta HIDS se pueden solucionar con facilidad. El primero se refiere a una pérdida de confidencialidad del sistema. En ese caso, los archivos de registro que informan al IDS pueden corromperse o ser imprecisos. Esto puede hacer que sea difícil determinar dónde recae la culpa o que el sistema no sea fiable. El segundo problema más importante que puede surgir con HIDS es que debe implementarse en cada sistema que lo necesite, lo cual puede convertise en un quebradero de cabeza para el personal técnico y administrativo.
Una de las mayores ventajas de HIDS es la posibilidad de guardar sumas de comprobación en los archivos. Estas pueden emplearse para informar a los administradores de que los archivos se han alterado durante un ataque. La recuperación se simplifica porque es más fácil determinar el lugar en el que se ha producido la manipulación.
Los IDS basados en host suelen responder de modo pasivo ante un incidente. En teoría, una respuesta activa podría ser similar a las que proporciona un IDS basado en red.
<Nivel 2>Trabajar con NIPS
<Cuerpo texto>Al contrario que los NIDS, el objetivo de los NIPS (*Network Intrusion Prevention Systems*, Sistema de revención de intrusión basado en red) es la prevención. Estos sistemas se centran en las concordancias de firma y, con posterioridad, determinan la forma de proceder. Por ejemplo, ante un posible ataque, los paquetes pueden eliminarse o ignorarse. Para ello, el NIPS tiene que detectar que está teniendo lugar un ataque . Por este motivo, se puede argumentar que NIPS es un subconjunto de NIDS.
<Nota>**Nota:** La línea existente entre las tecnologías sigue desdibujándose. Por ejemplo, en EE. UU NIST (*National Institute of Standards and Technology*, Instituto nacional de estándares y tecnología) se refiere ahora a sus publicaciones como IDPS (Intrusion Detection and Prevention Systems, Sistemas de detección y prevención de intrusos). Aunque es importante estar al día en la terminología del mundo real, tenga en cuenta que el examen está congelado en el tiempo y debería estar familiarizado con terminología más antigua para afrontar las preguntas del examen.
**********INICIO DE NOTA**********
<Nivel 3>Archivos de registro en Linux
<Nota>Hay una serie de registros para comprobar las entradas que pueden indicar una intrusión. Las más importantes que debería examinar son las que se enumeran a continuación:
*********NOTA AL MAQUETADOR PONER COMO COURIER NEGRITRA NO EN ARIAL LAS RUTAS EN NEGRITRA DE ABAJO**********
<Sep-med>* **var/log/faillog:** Abra la línea de comando y emplee la utilidad faillog para ver una lista de los intentos fallidos de autenticación de los usuarios.
* **var/log/lastlog:** Abra la línea de comando y emplee la utilidad lastlog para ver una lista de todos los usuarios que han iniciado sesión y cuándo fue la última vez que lo hicieron.
* **var/log/messages:** Use grep o un derivado thereof para encontrar entradas relacionadas con el acceso en este archivo.
* **var/log/wtmp:** Abra la línea de comando y emplee la utilidad last para ver una lista de usuarios que se ha autentificado en el sistema.
**********FIN DE NOTA**********
<Nivel 2>Utilizar honeypots
<Cuerpo texto>Un *honeypot* es un ordenador que se ha designado como destino de ataques informáticos. El mejor modo de visualizar este concepto es pensar en Winnie the Pooh y las muchas ocasiones en las que el personaje se

queda atrapado intentando sacar miel de las jarras. Al quedar atrapado, se incapacita a sí mismo y se convierte en un blanco fácil para todo aquel que quiera encontrarle.
<Nota>**Nota:** Dos de los *honeypot* más conocidos de Linux son *honeyd* (http://honeyd.org) y *Tiny Honeypot* (thp) (http://freshmeat.net/projects/thp/).
<Cuerpo texto>El objetivo de un *honeypot* es sucumbir a un ataque. Durante el proceso de agonía, puede utilizar el sistema para recopilar información sobre el desarrollo del ataque y los métodosque se han utilizado para establecerlo. Su principal ventaja es que dibuja al atacante fuera del verdadero sistema y permite a los administradores incrementar su capacidad en su estrategia de ataque. En la figura 3.9, pudo observar el diagrama de la implementación de un *honeypot*.
En general, los *honeypots* ni son seguros ni están bloqueados. Si viene de fábrica con un sistema operativo y software de aplicaciones, puede configurarlo así. Los sistemas *honeypots* que elabore pueden contener información y un software que atraigan a un atacante para que investigue en mayor profundidad y tome el mando del sistema. Si no se configura de forma adecuada, un sistema *honeypot* puede utilizarse para lanzar ataques contra otros sistemas.
Hay muchas iniciativas en este ámbito. Una de las más interesantes es el proyecto Honeynet Project, que creó una red sintética que se puede ejecutar en un único sistema informático y se adjunta a una red normal que utiliza una NIC. El sistema parece una red corporativa completa con aplicaciones y datos, pero todos ellos son falsos. Como parte de Honeynet Project, la red se escanea con frecuencia, se insertan gusanos y se intenta contactar con otros sistemas para infectarlos, todo en el curso de tres días. El último día, el sistema se infecta con no menos de tres gusanos. Esta plaga se produce sin que Honeynet Project lo anuncie.
<Nota>**Nota:** Encontrará información adicional en Honeynet Project (http://www.honeynet.org/).
<Cuerpo texto>Antes de barajar la posibilidad de implementar un proyecto del tipo *honeypot* o *honeynet*, es necesario que entienda los conceptos de incentivo e incitación:
<Sep-med>* **Incentivo:** Proceso para atraer a alguien a su plan o trampa. Puede conseguirlo anunciando un software gratuito o alardeando de que nadie ha conseguido irrumpir en su máquina. Si invita a alguien a que lo intente, está tentando a que hagan lo que quiere.
* **Incitación:** Proceso por el que un oficial de las fuerzas del orden o un agente del gobierno anima o induce a una persona a cometer un delito cuando el presunto delincuente expresa el deseo de no seguir adelante. La incitación es una defensa legítima en una investigación penal.
<Cuerpo texto>El incentivo es legal pero la incitación no. Es probable que sus responsabilidades legales sean pequeñas en cualquier caso, pero debería buscar asesoramiento jurídico antes de implementar un *honeypot* en su red. Puede que también le interese ponerse en contacto con las fuerzas de orden público o con la fiscalía si quiere iniciar acciones legales contra los atacantes.
<Nota>**Nota:** Algunos expertos en seguridad utilizan el término *tar pit* (pozo de brea) en lugar de *honeypot*. Ambos se pueden intercambiar entre sí.
<Nivel 1>Analizadores de protocolo
<Cuerpo texto>Los términos analizador de protocolo y examen de paquetes son intercambiables. Ambos se refieren al proceso de monitorización de datos que se transmiten a través de la red. El software que ejecuta la operación se llama analizador o *sniffer*, como hemos mencionado con anterioridad. Los *sniffer* están disponibles en Internet. En un primer momento, estas herramientas se idearon para legitimar procesos de monitorización de red, pero también se pueden utilizar para recabar datos con propósitos ilegales.
Por ejemplo, el tráfico IM (*Instant Messaging*, Mensajería instantánea) usa Internet y es potencialmente útil para actividades de examinación de paquetes. Cualquier información que contenga una sesión IM puede ser interceptado. Asegúrese de que los usuarios entienden que no deberían enviar información confidencial empleando este método.
Una de las herramientas más conocidas para analizar el tráfico de red en tiempo real es Snort (http://www.snort.org). El ejercicio 3.1 describe la instalación de esta herramienta.
**********Inicio ejercicio**********
<Nivel 4>Ejercicio 3.1. Instalar Snort en Linux
<Cuerpo texto>El estándar que se utiliza para la detección de intrusiones en Linux es Snort. Para instalar el paquete en un servidor SuSE, siga estos pasos:
<Sep-med>1. Acceda como *root* e inicie YaST.
2. Seleccione **Software** y, a continuación, **Instalar y eliminar software**. Busque **snort**.
3. Seleccione la casilla de verificación cuando aparezca el paquete.
4. Haga clic en **Aceptar**. Si aparecen mensajes de dependencia, haga clic en **Continuar** para añadirlos también.
5. Cambie los CD cuando se le pida y salga de YaST cuando se haya completado.
<Cuerpo texto>Para utilizar Snort, abra una sesión de terminal y escriba **snort**. Esto genera un mensaje de error que enumera todas las opciones que puede utilizar.
**********fin ejercicio**********
<Nivel 1>Asegurar terminales y servidores
<Cuerpo texto>Los terminales son muy vulnerables en una red. La mayoría de los terminales externos, con independencia de su sistema operativo, se comunican mediante servicios como uso compartido de archivos, servicios de red y programas de aplicaciones. Muchos de estos programas ofrecen la posibilidad de conectarse a otros terminales o servidores.
<Nota>**Truco:** Debido a que la red suele consistir en una cantidad mínima de servidores y un gran número de terminales, para un *hacker* es más sencillo encontrar un terminal inseguro y acceder a él, en primer lugar. Una vez que haya entrado en el terminal, resulta más fácil introducirse en la red, ya que, de ese modo, estaría dentro del cortafuegos.

<Cuerpo texto>Estas conexiones pueden ser vulnerables a la interceptación y explotación. El proceso para conseguir que un terminal o servidor sea más seguro se llama endurecimiento de la plataforma. Por su parte, el proceso de endurecer el disco duro se conoce como endurecimiento del SO (este forma parte del endurecimiento de la plataforma, pero solo trata el sistema operativo). Los procedimientos para endurecer la plataforma se clasifican en tres áreas básicas:
<Sep-med>* **Eliminación:** Eliminar software, servicios y procesos que no se utilizan del terminal (por ejemplo, quitar el servicio de un servidor), ya que pueden crear oportunidades de explotación.
* **Actualización:** Comprobar que todos los servicios y aplicaciones están actualizados (incluyendo los servicios disponibles y los paquetes de seguridad) y configurados del modo más seguro posible. Esto puede incluir contraseñas asignadas, acceso limitado y capacidades restringidas.
* **Minimización:** Reducir la diseminación de la información sobre el sistema operativo, los servicios y las capacidades del sistema. Muchos ataques pueden dirigirse a plataformas específicas, una vez que han sido identificadas. Muchos sistemas operativos usan nombres de cuenta predeterminados para el acceso administrativo. Siempre que sea posible, debería cambiar todo esto. Durante una nueva instalación de Windows 7 o Windows Vista, el primer usuario que se crea se añade de forma automática al grupo Administradores. Windows va un paso más allá y deshabilita de forma automática la cuenta actual del administrador, una vez que se haya creado otra cuenta que pertenezca al grupo Administradores. Versiones anteriores de Windows no lo hacían y la cuenta seguía habilitada. En Linux la cuenta de usuario *root* también se crea de forma automática durante la instalación.
<Nota>**Truco:** Una forma de evitar que los usuarios modifiquen el sistema operativo de Microsoft es bloquear sus opciones de configuración. Esto es posible con clientes Windows mediante el uso de políticas de grupo.
<Cuerpo texto>La mayoría de productos de servidor modernos también ofrecen una funcionalidad de terminal. De hecho, muchos servidores son casi imposibles de distinguir de los terminales. En ocasiones, Linux funciona como terminal y servidor.
Gran parte de los ataques exitosos contra servidores también funcionan con un terminal y viceversa. De forma adicional, los servidores ejecutan aplicaciones específicas, como SQL Server o un servidor Web de función completa.
<Nota>**Nota:** Una versión anterior de IIS (*Internet Information Services*, Servicios de información de Internet) incluía un sistema de correo electrónico predeterminado como parte de su instalación. Este sistema quedaba instalado a menos que se deshabilitara expresamente. Este sufría la mayoría de vulnerabilidades ante infecciones de virus y gusanos que hemos tratado con anterioridad. Compruebe que su sistema solo ejecuta los servicios, protocolos y procesos que necesita. Desactive o deshabilite todo aquello que no necesite.
<Cuerpo texto>Cuando esté buscando métodos para endurecer un servidor, nunca infravalore lo obvio. Siempre debería aplicar todas las revisiones y correcciones que se hayan publicado para el sistema operativo. Además, debería comprobar que no está ejecutando ningún servicio que sea innecesario.
**********INICIO DE NOTA**********
<Nivel 3>Los usuarios instalan software no autorizado
<Nota>Los miembros de su departamento IS (*Information Systems*, Sistemas de información) están molestos por la cantidad de software no autorizado que se está instalando en muchos de los clientes Windows de su red. Por ello, le piden consejo sobre cómo minimizar el impacto de este software. ¿Qué les diría?
Todos los clientes más nuevos de Windows admiten que se establezcan permisos para evitar instalaciones de software. Asimismo, debería evaluar las capacidades de los ajustes en el terminal por cuestiones de seguridad. Este proceso se conoce como bloqueo del escritorio. Gracias a él conseguirá bloquear la mayoría de escritorios y evitar la instalación de software. Aunque esto parezca una excelente solución, recuerde que hacerlo también impedirá que los usuarios puedan actualizar el software de forma automática. Esto aumentará, probablemente, el volumen de trabajo del departamento IS. Por este motivo, tendrá que sopesar las dos opciones y determinar cuál es la más adecuada y, a continuación, hacer su recomendación al departamento IS.
**********FIN DE NOTA**********
**********INICIO DE NOTA**********
<Nivel 3>Encontrar modos de endurecer sus servidores
<Nota>Armado con una lista de los distintos tipos de servidor de su red, busque formas de endurecerlos respondiendo a las siguientes preguntas:
<Sep-med>1. ¿Se están ejecutando servicios innecesarios?
2. ¿Tiene las últimas revisiones y actualizaciones instaladas?
3. ¿Hay cuestiones relacionadas con el sistema operativo?
4. ¿Hay cuestiones relacionadas con servicios o aplicaciones que está ejecutando?
<Nota>Una de las primeras tareas que debe realizar es dirigirse a un motor de búsqueda e introducir la palabra **endurecimiento** junto con el sistema operativo exacto que está utilizando.
**********FIN DE NOTA**********
<Nivel 1>Asegurar conexiones a Internet
<Cuerpo texto>Internet es, quizás, el área de mayor crecimiento para las redes. La tecnología empezó como un proyecto de investigación fundado por el Departamento de Defensa de EE. UU. y ha crecido de forma vertiginosa. Dentro de algunos años, se espera que casi todos los ordenadores del mundo estén conectados a Internet. Esta situación es una pesadilla, en lo que a seguridad se refire, y es una de las principales razones por las que se espera que la demanda de profesionales formados en seguridad de la información y en informática se multiplique de forma exponencial.
Las siguientes secciones describen los puertos y *sockets* y, con posterioridad, algunos de los protocolos más comunes, incluyendo correo electrónico, Web y FTP. Debería estar familiarizado con todos ellos para el examen.
<Nivel 2>Trabajar con puertos y sockets

<Cuerpo texto>Como ya hemos mencionado, el principal método de conexión entre sistemas a través de Internet es TCP/IP. Este protocolo establece conexiones y circuitos usando una combinación de direcciones IP y un puerto. El puerto es una interfaz que utiliza para conectar un dispositivo. Los *sockets* son la combinación de la dirección IP y el puerto. Por ejemplo, si intenta conectarse a un sistema remoto con la dirección 192.168.0.100, que está ejecutando un sitio Web, usará el puerto 80 de forma predeterminada. La combinación de estos dos elementos es un *socket*. La dirección completa y la descripción del *socket* sería 192.168.0.100:80.
IP se utiliza para redirigir la información de un host a otro a través de una red. Las cuatro capas de TCP/IP encapsulan la información en un paquete IP válido que, con posterioridad, se transmite a través de la red. La figura 3.11 ilustra los componentes clave de un paquete TCP solicitando la página de inicio de un sitio Web. Se devolverán los datos desde el sitio Web al puerto 1024 en el host originario.
**********3_011.tif**********
<Pie figura>**Figura 3.11.** Paquete TCP solicitando la página de inicio de un servidor Web.
<Cuerpo texto>El puerto de origen es al que se dirige en el destino. El puerto de destino es al que se envían los datos. En el caso de una aplicación Web, los datos de las dos direcciones de puerto contendría 80. En este paquete, TCP utiliza diferentes campos por cuestiones de verificación e integridad, pero no tiene que preocuparse por ello de momento.
Sin embargo, el campo de datos contiene el valor Get/. Este requiere la página de inicio del servidor Web. En resumen, este comando o proceso solicitó la página de inicio del sitio 192.168.0.100 puerto 80. Los datos se forman en otro paquete de datos que se pasan al IP y se envían de vuelta al sistema originario en el puerto 1024.
Las conexiones a la mayoría de servicios que usan TCP/IP se basan en este modelo de puerto. Muchos de los puertos están bien documentados y los protocolos para comunicarse con ellos son muy conocidos. Si un vendedor tiene una debilidad tecnológica o implementa una seguridad insuficiente, la vulnerabilidad se conocerá y se sacará partido de ella en poco tiempo.
<Nivel 2>Trabajar con correo electrónico
<Cuerpo texto>El correo electrónico es una de las aplicaciones más populares que se utilizan en Internet. Hay muchos servidores y clientes de correo electrónico buenos disponibles. La figura 3.12 muestra el proceso para transferir un mensaje de correo electrónico.
**********3_012.tif**********
<Pie figura>**Figura 3.12.** Conexiones de correo electrónico entre clientes y un servidor.
<Cuerpo texto>Los sistemas de correo electrónico más comunes utilizan los siguientes protocolos que, a su vez, emplean TCP para el establecimiento de sesión:
<Sep-med>* **SMTP:** Protocolo de entrega de correo electrónico que se utiliza para enviar correos electrónicos entre un cliente y un servidor, así como entre servidores. Los mensajes pasan del cliente al servidor a través de Internet. Cada mensaje puede tomar una ruta diferente desde el cliente al servidor. En el caso de la figura 3.12, los clientes están en dos servidores de correo electrónico diferentes, pero podrían estar en el mismo y el proceso sería transparente para el usuario. SMTP utiliza el puerto 25 y TCP para las conexiones.
* **POP:** Protocolo más reciente que se basa en SMTP para la transferencia de mensajes con el propósito de recibir correo electrónico. POP proporciona un almacenamiento de mensaje que puede utilizarse para guardar y reenviar correos. Si un servidor no está operativo, el servidor de origen puede almacenar un mensaje e intentar restablecerlo más tarde. POP3, la versión más actual de POP, permite que los mensajes se transfieran desde la oficina de correos en espera al cliente. El estándar POP actual usa el puerto 109 para POP2 y 110 para POP3. POP usa TCP para las conexiones.
* **IMAP (*Internet Message Access Protocol*, Protocolo de acceso a mensajes de Internet):** Es el reproductor más reciente en el campo del correo electrónico y se está convirtiendo rápidamente en el más conocido. Al igual que POP, IMAP tiene la capacidad de almacenamiento y reenvío. No obstante, tiene muchas más funcionalidades: permite que los mensajes se guarden en un servidor de correo electrónico, en lugar de que se descarguen para el cliente, y descarga mensajes basándose en criterios de búsqueda. Por otro lado, muchas implementaciones IMAP pueden realizar conexiones usando navegadores Web. La versión actual de IMAP (IMAP 4) usa el puerto 143 y TCP para conexiones.
<Nota>**Nota:** S/MIME y PGP son dos de los métodos más conocidos para proporcionar seguridad. Los trataremos en siguientes capítulos.
<Nivel 2>Trabajar con la Web
<Cuerpo texto>Cuando dos host se comunican a través de la Web, los datos se devuelven desde el host usando HTML, que no es más que un esquema de código para permitir que el texto y las imágenes estén presentes de un modo específico en un navegador Web. Puede crear HTML de varias formas, incluso a través del código manual y en programas de diseño gráfico. Su navegador lee e interpreta los archivos HTML y los visualiza en su sistema. Si quiere comprobar el aspecto del HTML, puede configurar el navegador para ver el código fuente. Verá cosas similares a codificación de un procesador de texto para casi todas las características de la página Web que está observando.
Los sitios Web son colecciones de estas páginas a las que puede llamar con su navegador cuando hace clic en un enlace o navega entre las páginas. La mayoría de los desarrolladores quieren algo más que la posibilidad de mostrar páginas y texto coloreado en su ordenador. Para la creación de sitios Web creativos y sofisticados, los navegadores Web se han ido haciendo más complejos, así, por ejemplo, poseen servidores Web. Ahora los navegadores incluyen audio, vídeos, animaciones, chats dinámicos y casi cualquier otra característica que pueda imaginar.
La figura 3.13 ilustra parte del contenido que puede enviar por Internet a través de un servidor Web.
**********3_013.tif**********
<Pie figura>**Figura 3.13.** Un servidor Web proporcionando flujo de vídeo, animación y datos HTML a un cliente.

<Cuerpo texto>La habilidad de enviar contenido a través de la Web se puede conseguir de varias formas. El enfoque más común implica instalar aplicaciones que se comunican mediante el servidor a su navegador. Dichas aplicaciones requieren que se abran puertos adicionales en el cortafuegos y los enrutadores. Por desgracia, hacer esto crea, de forma inherente, vulnerabilidades de seguridad.
<Nota>**Nota:** Cada puerto que se abre en la red incrementa la vulnerabilidad. Por ejemplo, si abre los puertos necesarios para utilizar el conocido programa Net-Meeting, está exponiendo a los usuarios a oportunidades de ataque adicionales. NetMeeting, como muchos otros programas, ha tenido una serie de vulnerabilidades en el pasado y es probable que se enfrente a más en el futuro.
<Cuerpo texto>Los conocidos servicios Web se ofrecen en combinación con programas habilitados para Web, como Flash y Java. Éstos utilizan un *socket* para comunicarse o un programa que responda a comandos a través del navegador. Si su navegador está controlado por una aplicación, su sistema correrá el riesgo de proporcionar datos que no quiera a los atacantes. Los servidores también son vulnerables a esta cuestión, ya que deben procesar solicitudes de navegadores pidiendo información o datos. Investigar las vulnerabilidades de un nuevo servicio propuesto pueden ahorrarle mucho tiempo más adelante si se convirtiera en el blanco de un ataque.
<Nota>**Nota:** Aunque HTML sigue siendo popular, XML (*Extensible Markup Language*, Lenguaje de marcado extensible) también se está haciendo su hueco. Pese a no ser un sustituto de HTML, XML proporciona muchas capacidades que el otro no ofrece, entre ellas, la habilidad de describir información (y no solo visualizarla). Al describir los datos, puede mostrarlos a través de varias plataformas o sistemas, por ejemplo.
<Cuerpo texto>La mejor solución para muchas de las vulnerabilidades que existen en la Web es implementar conexiones seguras, tema que se aborda en el siguiente apartado.
<Nivel 3>Conexiones Web seguras
<Cuerpo texto>Hay dos formas de proporcionar conexiones seguras entre un cliente y un servidor Web:
<Sep-med>* **SSL (*Secure Sockets Layer*, Capa de zócalo seguro) y TLS (*Transport Layer Security*, Seguridad de la capa de transporte):** Son dos protocolos que se suelen utilizar para transmitir información entre un cliente y un servidor Web. El SSL usa un esquema de cifrado entre los dos sistemas. El cliente inicia la sesión, el servidor responde, indicando que el cifrado es necesario, y, a continuación, negocian un esquema de encriptado adecuado. TLS es un protocolo más reciente que combina SSL con otros protocolos para proporcionar cifrado. TLS admite conexiones SSL por cuestiones de compatibilidad, pero también permite otros protocolos de cifrado, como Triple DES (*Data Encryption Standard*, Estándar de cifrado de datos). SSL/TLS usa el puerto 443 y TCP para las conexiones.
* **HTTP/S (*HTTP Secure*, HTTP Seguro):** Protocolo utilizado para conexiones seguras entre dos sistemas que usan la Web. Protege la conexión y todo el tráfico entre los dos sistemas está cifrado. HTTP/S usa SSL o TLS para conexiones seguras y usa el puerto 443 y TCP para las conexiones.
<Nota>**Nota:** No confunda S-HTTP (Secure HTTP) con HTTP/S. El primero es un protocolo diferente que permite a los sistemas negociar una conexión cifrada entre ambos. S-HTTP puede proporcionar alguna de las capacidades de HTTP/S, pero no es tan seguro y no se suele utilizar mucho. No obstante, es excelente para una pregunta de examen.
<Nivel 3>Vulnerabilidades de los complementos Web
<Cuerpo texto>El crecimiento de la Web y la demanda de más características por parte de los usuarios han motivado la creación de un nuevo conjunto de vulnerabilidades que deben evaluarse y gestionarse. Cada vez más, los navegadores Web y otras tecnologías con acceso a Internet permiten a los servidores enviar instrucciones al cliente para proporcionar capacidades multimedia. Dicha situación está creando un problema de cara a los profesionales de la seguridad, ya que estos protocolos presentan algunas debilidades potenciales.
Los siguientes apartados describen las aplicaciones habilitadas para Web más comunes, por ejemplo, JavaScript y subprogramas, así como las vulnerabilidades de las que debería ser consciente. Estas pueden incluir código malicioso, virus y explotaciones.
<Nivel 4>ActiveX
<Cuerpo texto>ActiveX es una tecnología implementada por Microsoft para personalizar controles, iconos y otras características, que incrementan la utilidad de sistemas habilitados para Web. ActiveX se ejecuta en el cliente. Para ello, utiliza un método para la seguridad llamado Authenticode, un tipo de tecnología de certificación que permite al servidor validar los componentes de ActiveX.
Los componentes de ActiveX se descargan en el disco duro del cliente, permitiendo posibles infracciones adicionales de la seguridad. Asimismo, los navegadores Web pueden configurarse para que requieran una confirmación antes de aceptar un control ActiveX. No obstante, muchos usuarios no entienden estos mensajes de confirmación cuando aparecen y aceptan de forma automática los componentes. Esto abre la oportunidad a posibles infracciones de la seguridad en el sistema de un cliente cuando se utiliza el control, ya que un control ActiveX puede contener instrucciones de programación que contengan código malicioso o crear vulnerabilidades en un sistema.
<Nota>**Nota:** Se recomienda que los navegadores estén configurados para no permitir que ActiveX se ejecute sin informar al usuario de las lagunas de seguridad que podría abrir.
<Nivel 4>Desbordamientos de búfer
<Cuerpo texto>Los desbordamientos de búfer se producen cuando una aplicación recibe más datos de los que está programada para aceptar. Esta situación puede provocar que una aplicación finalice o escribir datos más allá de los límites de espacio asignado. La conclusión puede dejar al sistema enviando los datos con un acceso temporal a niveles privilegiados en el sistema atacado, mientras que la sobrescritura puede causar que se pierdan datos importantes. Esta explotación suele ser el resultado de un error de programación en la implementación del software. Los desbordamientos de búfer siguen siendo bastante frecuentes y dista mucho de ser un pequeño problema, aunque eran una fuente de explotación menos frecuente en el pasado.
<Nivel 4>Interfaz de puerta de enlace común

<Cuerpo texto>La CGI (*Common Gateway Interface*, Interfaz de puerta de enlace común) es una forma antigua de automatización que se utilizaba en los inicios de los sistemas Web. Con las secuencias de comandos CGI se capturaban datos de un usuario con sencillos formularios. Sin embargo, no se suelen emplear mucho en los nuevos sistemas y están siendo sustituidos por Java, ActiveX y otras tecnologías.
Las secuencias de comandos CGI se ejecutan en el servidor Web e interactúan con el navegador del cliente. No obstante, CGI no suele estar muy bien visto en las nuevas aplicaciones debido a cuestiones de seguridad, pero todavía se sigue usando de forma generalizada en sistemas más antiguos. Las vulnerabilidades de CGI son el resultado de su habilidad innata para hacer aquello que se comunica. Si una secuencia de comandos CGI se escribe para causar estragos (o lleva código extra añadido por alguien con malas intenciones) y se ejecuta, su sistema sufrirá. La mejor protección ante una debilidad es no ejecutar aplicaciones escritas en CGI, aunque también puede optar por otras escritas en lenguajes más actuales siempre que sea posible.
<Nivel 4>Cookies
<Cuerpo texto>Las *cookies* son archivos de texto que un navegador mantiene en el disco duro del usuario para proporcionar una persistente y personalizada experiencia web para cada visita. Una *cookie* suele almacenar información sobre el usuario. Por ejemplo, puede contener el historial de un cliente con el fin de mejorar el servicio. Si una librería quiere saber cuáles son sus hábitos de compra y los últimos libros que ha visitado en su sitio Web, puede introducir esta información dentro de una *cookie* en su sistema. La próxima vez que vuelva a esta tienda, el servidor podrá leer su *cookie* y personalizarla. Las *cookies* también pueden utilizarse para marcar el tiempo de un usuario con el propósito de limitar su acceso. Una institución financiera puede enviar a su navegador una *cookie* una vez que se haya autenticado, tras leerla el servidordeterminará cuándo ha expirado una sesión.
Claro está, las *cookies* se consideran un riesgo porque pueden contener información personal que podría llegar a manos equivocadas. Así, hoy en día son muy valiosas para los publicistas. Una nueva variedad de *cookie*, conocida como *evercookie*, escribe datos para multiplicar las localizaciones y, así, hacer imposible eliminarlas por completo (véase http://samy.pl/evercookie/).
Si la seguridad es su mayor preocupación, la mejor protección es no permitir que las *cookies* se acepten. Casi todos los navegadores ofrecen la opción de habilitar o deshabilitar *cookies*. Si las habilita, puede elegir entre aceptarlas/rechazarlas todas o solo aquellas que procedan de un servidor de origen.
<Nivel 4>Filtro de scripts de sitios
<Cuerpo texto>Usando un lenguaje de secuencias de comando en el lado del cliente, un indeseable podría engañar a un usuario que visite su sitio y, a continuación, ejecute código de forma local. Esto se conoce como XSS (*Cross-Site Scripting*, Filtro de scripts de sitios). Por ejemplo, el usuario A puede recibir un mensaje comunicándole que tiene que modificar su cuenta XYZ, pero el enlace no procede realmente del sitio XYZ (estrategia de suplantación de identidad). Cuando hace clic en el enlace, una rutina JavaScript empieza a ejecutarse en su máquina. La secuencia de comandos se está ejecutando en el sistema del usuario A porque tiene sus permisos y puede empezar a hacer cosas como ejecutar rutinas malintencionadas para enviar, eliminar o alterar los datos.
La mejor protección contra el filtro de scripts de sitios es deshabilitar los scripts.
<Nivel 4>Validación de entrada
<Cuerpo texto>Siempre que un usuario deba proporcionar valores en una sesión, los datos introducidos deberían validarse. Sin embargo, muchos vendedores han sido presa de las vulnerabilidades de su código. En algunos casos, se han aceptado valores vacíos, y, en otros, han permitido el escalamiento de privilegios si se utilizaban ciertas contraseñas de puerta trasera.
La mejor protección contra las vulnerabilidades de validación de entrada es que los desarrolladores sigan las prácticas recomendadas y que siempre validen los valores introducidos. Como administrador, cuando conoce la vulnerabilidad de la validación de entrada en cualquier aplicación de su sistema, debería dejar de usarla de forma inmediata hasta que se publique e instale una nueva revisión.
<Nivel 4>Subprogramas Java
<Cuerpo texto>Un subprograma Java es una pequeña secuencia de comandos Java que se descarga desde un servidor a un cliente y, con posterioridad, se ejecuta desde el navegador. El navegador del cliente debe tener la capacidad de ejecutar subprogramas Java en una máquina virtual. Hoy en días, éstos se utilizan de forma generalizada en servidores Web y se están convirtiendo en una de las herramientas más populares para el desarrollo de sitios Web. Las aplicaciones habilitadas para Java pueden aceptar instrucciones programadas (secuencias de comandos Java) desde un servidor y controlar ciertos aspectos del entorno del cliente. Estas secuencias ejecutan en el cliente.
Los subprogramas se inician en un área restringida de la memoria llamada espacio aislado (*Sandbox*). Este limita el acceso del subprograma a zonas del usuario y a los recursos del sistema. Un subprograma ejecutado en el espacio aislado se considera seguro, lo que quiere decir que no intentará acceder a las áreas confidenciales del sistema. Los errores de la máquina virtual Java que ponga en funcionamiento las aplicaciones pueden permitir que algunos subprogramas se inicien fuera del espacio aislado. Cuando esto ocurre, el subprograma es inseguro y puede realizar operaciones maliciosas. Los atacantes de los sistemas del cliente suelen explotar esta debilidad. Desde el punto de vista del usuario, la mejor defensa es asegurarse de que solo ejecuta subprogramas de sitios que tengan buena reputación, con los que esté familiarizado. Desde el punto de vista del administrador, la mejor defensa es asegurarse de que ciertos programadores se adhieran a las directrices de programación cuando crean subprogramas.
<Nivel 4>JavaScript
<Cuerpo texto>JavaScript es un lenguaje de programación que permite acceder a los recursos del sistema que ejecuta un script. Una secuencia de comandos o script es un programa de autocontenido que puede iniciarse como un archivo ejecutable en muchos entornos. Estos scripts pueden interactuar con todos los aspectos de un sistema operativo, por ejemplo el lenguaje C de programación. Esto significa que, cuando se ponen en funcionamiento, las secuencias de

comandos de JavaScript pueden dañar los sistemas o enviar información no autorizada. JavaScript puede descargarse desde un sitio Web de Internet y ejecutarse.
<Nivel 4>Ventanas emergentes
<Cuerpo texto>Aunque desde un punto de vista técnico no son un complemento, las ventanas emergentes son frustrantes y arriesgadas. Se denomina ventana emergente a un sitio Web u otra instancia (ya sea una pestaña u otra ventana del navegador) que un usuario visita y se abre en primer plano (*popup*). Si se abre en segundo plano, se llama ventana sumergida (*popunder*). Las dos abren páginas o sitios que el usuario no solicitó de forma específica y puede que solo muestren anuncios, pero también pueden incorporar subprogramas no deseados.
Los bloqueadores de ventanas emergentes se utilizan para evitar que aparezcan las dos variedades. Aunque los navegadores más antiguos no incorporan una opción para este fin, los más recientes sí suelen incluir esta capacidad.
<Nivel 4>Subprogramas firmados
<Cuerpo texto>Los subprogramas firmados son similares a los subprogramas de Java pero con dos diferencias clave. Un subprograma firmado no se ejecuta en el espacio aislado de Java y tiene mayor capacidad para acceder al sistema. Además, no suelen descargarse de Internet. Este tipo de subprogramas suele provenir de esfuerzos internos o programación personalizada. También pueden incluir una firma digital para verificar su autenticidad. Si se autentica, se instalará. Los usuarios nunca deberían descargar subprogramas firmados, a menos que estén seguros de que el proveedor es de confianza. Un subprograma firmado procedente de un proveedor que no es de fiar conlleva los mismos riesgos de seguridad que un subprograma sin firmar.
<Nota>**Truco:** Una vulnerabilidad es asumir siempre que un subprograma es seguro porque está firmado. Aunque esté firmado, puede ejecutar tareas fuera del ámbito de los subprogramas normales, por ejemplo, iniciar programas. Un programador contrariado puede crear subprogramas firmados maliciosos y provocar estragos hasta que se le detenga.
<Cuerpo texto>La mayoría de navegadores Web tienen opciones que puede utilizar para controlar el acceso Java a los recursos usando subprogramas o secuencias de comandos Java.
<Nivel 4>Retransmisión SMTP
<Cuerpo texto>La retransmisión SMTP es una característica diseñada en muchos servidores de correo electrónico que les permite reenviar correos a otros servidores de correo. En un principio, esta función se ideó para servir de puente al tráfico entre sistemas. Esta capacidad hace posible que las conexiones de correo electrónico entre los sistemas a través de Internet se lleven a cabo con mayor facilidad.
Por desgracia, esta característica se ha utilizado para generar una gran cantidad de spam en Internet. Un sistema de correo electrónico que permite que se produzca este tipo de reenvío se conoce como retransmisión abierta. Los individuos que no tengan escrúpulos pueden usar estas retransmisiones para enviar publicidad y otros mensajes a través de los servidores de retransmisión abierta y publicar su servidor de correo en listas para que otros lo utilicen (lo que haría que su servidor estuviera en una lista negra). La retransmisión SMTP debería estar deshabilitada en su red, a noser que esté limitada a servidores de correo electrónico de su dominio.
<Nivel 2>Trabajar con Protocolo de Transferencia de Archivos
<Cuerpo texto>FTP ha sido el protocolo más utilizado para transferir archivos entre sistemas a través de Internet durante muchos años y está disponible en la mayoría de los principales entornos de servidor.
**********INICIO DE NOTA**********
<Nivel 3> Retransmisión SMTP en acción
<Nota>Imagine que acaba de recibir la llamada de un cliente comunicándole que su servidor de correo electrónico se está comportando de forma peculiar. Cuando llega al sitio, observa que hay más de 20.000 correos electrónicos en la carpeta de correo saliente y que el sistema no tiene espacio disponible en el disco. Cuando desactiva el software de correo electrónico, elimina estos archivos y reinicia el servidor. Acto seguido, se da cuenta de que la carpeta de correo saliente se está volviendo a llenar. ¿De qué problema podría tratarse?
Los vendedores por correo electrónico pueden usar el servidor como retransmisión. Este secuestro continuará hasta que deshabilite las capacidades de retransmisión SMTP en el servidor. Muchos sistemas antiguos no permiten que se desactive la retransmisión SMTP, por lo que dichos servidores tienen que actualizarse o sustituirse para evitar que esto continúe.
**********FIN DE NOTA**********
<Cuerpo texto>Internet ha sustituido muchas de las funciones de FTP antiguas. Ahora, FTP se utiliza de forma generalizada, pero va perdiendo popularidad debido a la aparición de otros métodos de descarga de archivos. Los navegadores más conocidos permiten acceder a un sitio FTP como a un sitio Web y HTTP es compatible con capacidades para transferir archivos. Un navegador proporciona una interfaz gráfica que pueden utilizar los usuarios sin tener que exponerse a la estructura de comandos que FTP proporciona de forma predeterminada.
Los siguientes apartados describen FTP, sus vulnerabilidades y los métodos para asegurarlo.
<Nivel 3>FTP ciego/anónimo
<Cuerpo texto>Los primeros servidores de FTP no ofrecían seguridad formal. Esta se basaba en el código de honor. En la mayoría de los casos, este se utilizaba estrictatamente para descargar archivos desde un servidor FTP a un cliente. Este último no podía subir archivos sin utilizar un ID de acceso diferente. En algunos casos, se daba la situación contraria y un cliente podía subir archivos "a ciegas" para que otros no pudieran descargar e incluso ver los archivos.
La mayoría de inicios de sesión en un FTP utilizaban el acceso anónimo. De forma convencional, el ID de inicio de sesión era anónimo y la contraseña era la dirección de correo electrónico del usuario. Este código de honor se sigue utilizando en sistemas que quieren permitir acceso público a archivos y simplifica la administración porque solo emplea una cuenta.

No obstante, el coste de esta implementación es el riesgo que conlleva. En esta circunstancia, la única seguridad que ofrece es la establecida por el sistema operativo.
<Nivel 3>FTP seguro
<Cuerpo texto>El FTP seguro (S/FTP o SFTP) se consigue usando un protocolo llamado SSH, un tipo de protocolo de túnel que permite el acceso a sistemas remotos de modo seguro. Como hemos mencionado con anterioridad, SSH permite que las conexiones sean seguras cifrando la sesión entre el cliente y el servidor. SSH está disponible para Unix y otros sistemas que proporcionan una capacidad similar a FTP.
<Nivel 3>Compartir archivos
<Cuerpo texto>El uso compartido de archivos se consigue almacenándolos en una localización asignada del servidor o un terminal. Cuando se almacenan en una terminal, la conexión se conoce como punto a punto. La localización asignada suele ser un subdirectorio de una de las unidades de disco del servidor o en otro terminal.
En una conexión FTP, puede subir un archivo desde un cliente usando el comando PUT. Descárguelo usando GET. La mayoría de las aplicaciones y servidores modernos permiten que el programa de una aplicación acceda a archivos compartidos a nivel de registro. Este tipo de uso compartido pone en funcionamiento aplicaciones multiusuario, por ejemplo, bases de datos. Los navegadores Web suelen aceptar archivos de un servidor Web descargándolos desde el servidor. Con posterioridad, dichos archivos se procesan a través del navegador y se muestran al usuario.
<Nivel 3>Vulnerabilidad del FTP
<Cuerpo texto>FTP tiene una brecha principal: el ID de usuario y la contraseña no están cifrados y están sujetos a la captura de paquetes. Esto crea una grieta en la seguridad muy importante, sobre todo, si está conectado a un servidor FTP a través de Internet. También habrá un problema si está permitiendo el uso de la versión anónima de FTP: TFTP, un servicio basado en UDP que no tiene nombre de usuario ni contraseña y puede utilizarse para transferir archivos en modo desatendido.
**********INICIO DE NOTA**********
<Nivel 3>Transferencia de archivos remotos
<Cuerpo texto>Su empresa tiene una gran cantidad de usuarios remotos que transfieren archivos a su sistema a través de Internet. Esta es una parte esencial de su negocio y tiene que seguir permitiéndolo. Quiere proporcionar una seguridad adicional a sus usuarios para que la información no pierda confidencialidad. ¿Cómo lo haría?
Podría implementar SSH u otros protocolos seguros para las transferencias de archivos mediante el FTP. Con ello, permitiría que se enviara información a través de Internet de modo seguro. También podría utilizar TLS, SSL u otro formato seguro.
**********FIN DE NOTA**********
<Nivel 1>Protocolos de red
<Cuerpo texto>Puede que su red tenga otros protocolos en ejecución además de TCP/IP y que cada uno de ellos pueda ser vulnerable a ataque externos. Algunos protocolos (como NetBEUI (*NetBIOS Extended User Interface*, Interfaz extendida de usuario de NetBIOS), DLC (*Data Link Control*, Control de enlace de datos y otros más primitivos) no son enrutables y, por lo tanto, no están sujetos a posibles ataques. Por supuesto, hay un gran "a menos que". Si el enrutador o el cortafuegos están configurados para pasarlos, algunos de estos protocolos pueden incrustarse en TCP/IP y transferirse a otros sistemas.
Los protocolos principales utilizados por TCP/IP para mantenimiento y otras actividades incluyen los que se describen en la siguiente lista:
<Sep-med>* **SNMP:** TCP/IP usa SNMP para gestionar y monitorizar dispositivos en una red. Muchas fotocopiadoras, máquinas de fax y otras máquinas de oficina inteligentes usan SNMP para funciones de mantenimiento. Este protocolo viaja bastante bien a través de los enrutadores y puede ser vulnerable a ataques. Pese a que este no sea peligroso, tenga en cuenta qué podría ocurrir si de repente su impresora se conecta y empieza a lanzar papel al suelo.
SNMP se actualizó como estándar SNMPv2, que proporciona seguridad y monitorización remota mejorada. SNMP se está revisando en este momento. Aunque se publique un nuevo estándar (SNMPv3), la mayoría de sistemas seguirán usando SNMPv2.
* **ICMP:** TCP/IP usa ICMP para informar de errores y contestar solicitudes de programas como Ping y Traceroute. Este es uno de los protocolos favoritos utilizado para ataques DoS. Muchas empresas han deshabilitado ICMP a través del enrutador para evitar que se produzcan este tipo de situaciones.
**********INICIO DE NOTA**********
<Nivel 3>Deshabilitar ICMP para gestionar ataques smurf
<Nota>Su empresa ha sufrido varios ataques *smurf* (un ataque que utiliza la suplantación del IP y la redifusión para enviar un *ping* a un grupo de host en una red). Dichos ataques han provocado grandes trastornos y deben detenerse. ¿Qué sugeriría para minimizar estos ataques?
Debería recomendar que se deshabilite el tráfico ICMP en el punto en el que la red se conecta a Internet. Para ello, puede deshabilitar el protocolo en el enrutador u bloquear este tráfico en los sistemas del cortafuegos. Con ello, no elimina el problema por completo, pero reduce en gran medida la posibilidad de que se produzca un ataque con éxito usando ICMP. Este paso también evitará el acceso a información sobre su red, ya que los programas (por ejemplo, Ping) que soliciten información desde sus sistemas de red ya no funcionarán.
**********FIN DE NOTA**********
<Sep-med>* **IGMP:** TCP/IP usa IGMP para gestionar sesiones de grupo o multidifusión. Puede emplearse para dirigir a varios receptores un paquete de datos: el remitente inicia el tráfico de difusión y los clientes que tengan esta capacidad habilitada lo reciben. (La difusión son mensajes enviados desde un único sistema a la totalidad de la red. Los sistemas no tienen por qué estar dentro de la red.) Este proceso, llamado multidifusión, puede consumir enormes cantidades de ancho de banda en una red y es posible que se cree una situación DoS. La mayoría de los

administradores de redes deshabilitan la recepción tráfico de difusión y multidifusión procedente del exterior de su red local.
Una unidifusión es tráfico IGMP orientado a un único sistema. TCP/IP utiliza sobre todo un método unidifusión de comunicación: un mensaje se envía de un sistema único a otro sistema único.
<Nota>**Nota:** Todos los protocolos principales que utiliza TCP/IP presentan un problema en potencia para los administradores de seguridad. Cerciórese de que utiliza lo que necesita y desactive lo que no.
<Nivel 1>Resumen
<Cuerpo texto>En este capítulo, hemos explicado los puertos y *sockets*. Estos últimos son el principal método que se utiliza para comunicarse con servicios y aplicaciones. Se pueden instalar para añadir configuraciones especiales y seguridad adicional.
Los monitores de red son herramientas esenciales para la resolución de problemas y pueden emplearse para husmear en las redes. Los sistemas para detectar intrusiones pueden adoptar un rol activo y controlar el tráfico y los sistemas. Los IDS usan procedimientos basados en reglas para comprobar los archivos de las auditorías y el tráfico de red, además pueden tomar decisiones basándose en estas reglas. En combinación con un cortafuegos, un IDS puede ofrecer un alto grado de seguridad.
<Nivel 1>Ideas clave para el examen
<Cuerpo texto>A continuación, incluimos las ideas clave que debe recordar para el examen Security+:
<Sep-med>* **Tecnologías usadas por TCP/IP e Internet:** Las direcciones IP y los números de puerto se combinan para crear una interfaz llamada *socket*. La mayoría de los protocolos TCP y UDP se comunican utilizando este *socket* como mecanismo de interfaz principal. Los clientes y los servidores se comunican a través de los puertos, los cuales pueden modificarse para mejorar la seguridad. Los servicios Web usan HTML y otras tecnologías para permitir sitios Web enriquecidos y vivos. Estas tecnologías pueden crear problemas de seguridad, ya que presentan vulnerabilidades individuales. Compruebe los problemas que existen desde la perspectiva de la seguridad antes de habilitar estas tecnologías en su sistema.
* **Principales métodos utilizados para monitorizar la red:** Los principales métodos para monitorizar la red son los *sniffers* y los IDS. Los primeros son pasivos y proporcionan una visualización en tiempo real del tráfico de red. En esencia, están ideados para la resolución de conflictos pero también son una de las herramientas más utilizadas por los atacantes para determinar qué protocolos y sistemas se están ejecutando. Los IDS son dispositivos activos que operan para alertar a los administradores de ataques y eventos inusuales. Esto se consigue revisando de forma automática los archivos de acceso y el tráfico del sistema, y aplicando reglas que dicten cómo reaccionar ante los eventos. Un IDS, cuando se utiliza en combinación con un cortafuegos, puede proporcionar una seguridad excelente para una red.
* **Los dos tipos de sistemas para detectar intrusiones en uso:** Los dos tipos de IDS que se utilizan son HIDS (y NIDS. Los IDS basados en host solo funcionan en el sistema en el que se instalan y los basados en la red monitorizan a sta en su totalidad.
* **Términos y funciones del entorno IDS:** Entre estos términos se incluyen actividad, administrador, alerta, analizador, fuente de datos, evento, supervisor, notificación, operador y sensor. Para mayor facilidad, algunos sistemas se combinan en los IDS, pero todas las funciones deben llevarse a cabo para que sean efectivos.
* **Diferencia entre una respuesta activa y una pasiva:** Una respuesta activa permite a un IDS gestionar los recursos de una red si se produce un incidente. Las respuestas pasivas implican la notificación y los informes de los ataques o actividades sospechosas.
* **Objetivo de un *honeypot*:** Sistema ideado para recopilar información o para ser destruida. Los sistemas *honeypot* sirven para conseguir pruebas en una investigación y para estudiar las estrategias de ataque.
<Nivel 1>Prueba de evaluación
<Sep-med>1. Para que una monitorización de red funcione de forma adecuada, necesita un PC y una tarjeta de red que funcione ¿en qué modo?
A. Lanzamiento. **B.** Exposición. **C.** Promiscuo. **D.** Barrido.
2. ¿Qué utilidad de Linux puede mostrar si hay más de un conjunto de documentación en el sistema para un comando del que está intentando encontrar información?
A. Lookaround. **B.** Howmany. **C.** Whereall. **D.** Whatis.
3. En el contexto de los sistemas para la detección de intrusiones, qué cuenta es responsable de establecer la política de seguridad de una empresa?
A. Supervisor. **B.** Administrador. **C.** Raíz. **D.** Director.
4. ¿Cuál de los siguientes sistemas de IDS busca cosas fuera de lo particular?
A. Basado en incongruencias. **B.** Basado en la varianza. **C.** Basado en anomalías. **D.** Basado en diferencias.
5. ¿Cuál de las siguientes opciones copia el tráfico de todos los puertos a un único puerto y no permite el tráfico bidireccional en él?
A. Expansión de puertos. **B.** Combinación de *sockets*. **C.** Fusión. **D.** Amalgama.
6. ¿Cuál de las siguientes opciones implica ignorar un ataque y suele ser una respuesta frecuente?
A. Abstención. **B.** Rechazo. **C.** Negación. **D.** Elusión.
7. ¿Qué sistema de IDS usa algoritmos para analizar el tráfico que pasa a través de la red?
A. Aritmético. **B.** Algebraico. **C.** Estadístico. **D.** Heurístico.
8. ¿Cuál de las siguientes utilidades puede utilizarse en Linux para ver una lista de usuarios que han fallado en su intento de autenticación?
A. Badlog. **B.** Faillog. **C.** Wronglog. **D.** Killlog.

9. ¿Cuál de los siguientes es el proceso por el que un oficial de las fuerzas del orden o un agente del gobierno anima o induce a una persona a cometer un delito cuando el presunto delincuente expresa el deseo de no seguir adelante?
A. Incentivo. **B.** Incitación. **C.** Engaño. **D.** Sarcasmo.
10. ¿Cómo se conoce la consola del IDS?
A. Supervisor. **B.** Ventana. **C.** Escritorio. **D.** Pantalla.
11. Los *sockets* son una combinación de la dirección IP y ¿cuál de los siguientes elementos?
A. Puerto. **B.** Dirección MAC. **C.** Opción NIC. **D.** ID de NetBIOS.
12. ¿Qué tipo de respuesta activa hace pensar al atacante que se está produciendo el ataque mientras el sistema monitoriza la actividad y redirige al atacante a un sistema que ha sido diseñado para destruirse?
A. Pretexto. **B.** Mentira. **C.** Engaño. **D.** Timo.
13. ¿Qué dispositivo monitoriza el tráfico de red de modo pasivo?
A. *Sniffer*. **B.** IDS. **C.** Cortafuegos. **D.** Navegador Web.
14. La seguridad se ha convertido en la mayor prioridad de su organización. Ya no le basta con reaccionar ante los ataques cuando se produzcan, quiere empezar a actuar de una forma más proactiva. ¿Qué sistema realiza una monitorización y un análisis de red más activo y puede tomar medidas proactivas para proteger una red?
A. IDS. **B.** *Sniffer*. **C.** Enrutador. **D.** Conmutador.
15. ¿Cuál de las siguientes opciones puede emplearse para monitorizar la actividad no autorizada de una red? (Elija dos opciones.)
A. *Sniffer* de red. **B.** NIDS. **C.** HIDS. **D.** VPN.
16. Usted es el administrador de Acme Widgets. Tras asistir a un congreso sobre cuestiones de gestión, su jefe le comunica que tiene que establecer un IDS y ponerlo en funcionamiento a finales de semana. ¿Cuál de los siguientes sistemas debería instalar en un host para proporcionar las capacidades de un IDS?
A. *Sniffer* de red. **B.** NIDS. **C.** HIDS. **D.** VPN.
17. ¿Cuál de las siguientes opciones es una respuesta activa en un IDS?
A. Enviar una alerta a una consola. **B.** Elusión. **C.** Volver a configurar un enrutador para bloquear una dirección IP. **D.** Hacer una entrada en el archivo de auditorías de seguridad.
18. Un administrador inexperto irrumpe en su oficina con un informe en las manos. Afirma que ha encontrado documentación que revela que un intruso ha estado entrando en la red con frecuencia. ¿Cuál de las siguientes implementaciones de IDS detecta intrusiones basándose en reglas establecidas con anterioridad en su red?
A. MD-IDS. **B.** AD-IDS. **C.** HIDS. **D.** NIDS.
19. ¿Qué función IDS evalúa los datos recopilados por los sensores?
A. Operador. **B.** Supervisor. **C.** Alerta. **D.** Analizador.
20. ¿Cómo se llama el sistema ideado o diseñado para que lo rompa un atacante?
A. *Honeypot*. **B.** *Honeybucket*. **C.** Señuelo. **D.** Sistema de parodia.
<Nivel 1>Respuestas de la prueba de evaluación
<Sep-med>1. C. Para que una monitorización de red funcione de forma adecuada, necesita un PC y una tarjeta de red que funcione en modo promiscuo.
2. D. En Linux, la utilidad whatis puede mostrar si hay más de un conjunto de documentación en el sistema para un comando del que está intentando encontrar información.
3. B. El administrador es la persona/cuenta responsable de establecer la política de seguridad de una empresa.
4. C. Un IDS basado en la detección de anomalías (AD-IDS) busca anomalías, es decir, cosas fuera de lo normal.
5. A. La expansión de puertos (también conocida como reflejo de puertos) copia el tráfico de todos los puertos a un único puerto y no permite el tráfico bidireccional en él.
6. D. Eludir o ignorar un ataque suele ser una respuesta frecuente
7. D. Un sistema heurístico usa algoritmos para analizar el tráfico que pasa a través de la red
8. B. Use la utilidad faillog en Linux para ver una lista de usuarios que ha fallado en su intento de autenticación.
9. B. La incitación es el proceso por el que un oficial de las fuerzas del orden o un agente del gobierno anima o induce a una persona a cometer un delito cuando el presunto delincuente expresa el deseo de no seguir adelante
10. A. La consola del IDS se conoce como supervisor.
11. A. Los *sockets* son una combinación de la dirección IP y el puerto.
12. C. El engaño es la respuesta activa que hace pensar al atacante que se está produciendo el ataque mientras el sistema monitoriza la actividad y redirige al atacante a un sistema que ha sido diseñado para destruirse.
13. A. Los analizadores de protocolo (*sniffers*) monitorizan el tráfico de red en tiempo real. También conocidos como monitores de red, se idearon en un principio para el mantenimiento y la resolución de conflictos en las redes.
14. A. Un IDS se utiliza para proteger y comunicar anomalías de red al administrador o al sistema. Funciona con archivos de auditoría y procesamiento basados en reglas para determinar cómo actuar en caso de que se produzca una situación inusual en la red.
15. A, B. Los *sniffers* de red y los NIDS se utilizan para monitorizar el tráfico de red. Los *sniffers* de red se gestionan de forma manual y los NIDS pueden automatizarse.
16. C. Un IDS basado en host (HIDS) se instala en los host que necesitan capacidades IDS.
17. C. Cambiar de forma dinámica la configuración del sistema para proteger una red o un sistema es una respuesta activa.
18. A. Comparando las firmas de ataque y las auditorías, un IDS de mal uso determina si se está produciendo un ataque.
19. D. La función analizador utiliza fuentes de datos recopilados por los sensores para analizar y determinar si se ha producido un ataque.

20. A. Un *honeypot* es un sistema ideado para sacrificarse en nombre del conocimiento. Los sistemas *honeypot* permiten a los investigadores evaluar y analizar las estrategias de ataque utilizadas. Los responsables de hacer cumplir la ley usan *honeypots* para recopilar pruebas en una investigación.

Capítulo 5. Control de acceso y gestión de identidad

<Cuerpo texto>En este capítulo se tratan los siguientes objetivos del examen CompTIA Security+:
<Sep-med>1.2 Aplicar e implementar principios de administración de red seguros.
1.3 Distinguir y diferenciar elementos y compuestos de red.
3.2 Analizar y diferenciar los tipos de ataque.
5.1 Explicar la función y el propósito de los servicios de autentificación.
5.2 Explicar los conceptos fundamentales y las prácticas más adecuadas en relación con la autentificación, la autorización y el control de acceso.
<Cuerpo texto>Los temas anteriores se han centrado más en conceptos teóricos que en componentes de compra. No obstante, han sentado las bases para las materias que ocupan el objeto de este capítulo. En este, la explicación está más orientada a la implementación de características de seguridad, en lugar de centrarse en los posibles problemas que puedan acontecer. Tenga en cuenta que, aunque exista una gran variedad de productos para satisfacer las necesidades del mercado, ninguna resultará un éxito sin la educación y formación adecuada. Una de sus principales prioridades siempre debería ser conseguir que los usuarios entiendan todos los aspectos de las políticas de seguridad. El presente capítulo empieza analizando las bases del control de acceso y, más adelante, explica en qué consisten el acceso remoto y los servicios de autenticación. Para concluir, examina la implementación del control de acceso y cuáles son las prácticas recomendadas.
<Nivel 1>Control de acceso básico
<Cuerpo texto>El control de acceso significa dejar entrar a los usuarios correctos (a los que están autorizados) y mantener fuera a los demás (a los que no están autorizados). Puede emplear una gran variedad de herramientas para conseguirlo (hablaremos de todas ellas en este capítulo) pero el principio fundamental sigue siendo el mismo: dejar a los correctos dentro.
En las siguientes secciones, analizaremos la diferencia entre identificación y autenticación, autenticación y autorización, y autenticación de factor múltiple y seguridad operativa. También describiremos los *tokens* y los problemas que tiene que afrontar, así como algunas cuestiones que debe considerar.
<Nivel 2>Identificación versus autenticación
<Cuerpo texto>Para responder de forma correcta a las preguntas del examen Security +, es esencial entender la diferencia entre identificación y autenticación. La identificación requiere que un humano interceda y verifique que alguien es quien dice ser. Este suele adoptar la forma de un guardia o recepcionista, ya que comprueba las credenciales que proporciona el usuario (por ejemplo, carnet de conducir, tarjeta de identificación de empleado, etc.) y confirma que pertenece a la persona que la está procesando.
La autenticación no es una prueba tan precisa ya que elimina el elemento humano del proceso de verificación y se limita a corroborar que el usuario ha introducido los valores correctos, como la contraseña que acompaña al nombre de usuario introducido. Con la autenticación, el usuario puede no ser quien dice ser, pero tiene la combinación correcta de valores (nombre de usuario y contraseña, *tokens*, biometría) y, por esta razón, se autentifica.
<Nota>**Truco:** Para el examen, recuerde que autenticación significa que alguien tiene información precisa, mientras que la identificación se refiere a que se demuestra que la información precisa está en posesión del individuo correcto.
<Cuerpo texto>Los sistemas o métodos de autenticación se basan en uno o más de los siguientes factores:
<Sep-med>* Algo que sabe, como una contraseña o clave.
* Algo que tiene, como una tarjeta inteligente, un símbolo o un dispositivo de identificación.
* Algo que es único en usted desde el punto de vista físico, como su huella o patrón de retina.
<Cuerpo texto>Los sistemas se autentifican unos a otros empleando métodos similares. Con frecuencia, los sistemas se pasan información privada para establecer la identidad. Una vez que ha tenido lugar la autenticación, los dos sistemas pueden comunicarse según el modo especificado en el diseño.
Es habitual que se utilicen muchos métodos comunes para la autenticación. Éstos se clasifican en las categorías de factor único y factor múltiple. Cada uno de ellos aporta algo a la seguridad y debería tenerlos en cuenta cuando evalúe los esquemas o métodos de autenticación.
<Nivel 2>Autenticación (factor único) y autorización
<Cuerpo texto>La forma más básica de autenticación se conoce como SFA (*Single Factor Authentication*, Autenticación de factor único) porque solo se comprueba un conjunto de valores. SFA se suele implementar como la combinación habitual de nombre de usuario/contraseña. Éstos son identificadores únicos de un proceso de inicio de sesión. En resumen, el funcionamiento sería el siguiente: cuando los usuarios se sientan delante de un sistema informático, lo primero que requiere el sistema de seguridad es que determine quién es.
La identificación se suele confirmar a través de un proceso de inicio de sesión. La mayoría de sistemas operativos utilizan un ID de usuario y una contraseña para ello. Estos valores pueden enviarse a través de la red como texto simple, pero también pueden estar cifrados.
El proceso de inicio de sesión identifica el sistema operativo y es posible que la red, haciéndole saber que el usuario es quien dice ser. La figura 5.1 ilustra este proceso de acceso y contraseña. Observe que el sistema operativo compara esta información con la que tiene almacenada en el procesador de seguridad y acepta o rechaza el intento de inicio de sesión. Por otro lado, dicho sistema puede establecer privilegios o servicios basándose en los datos almacenados de un ID en particular.
**********5_001.tif**********
<Pie figura>**Figura 5.1.** Se está llevando a cabo un proceso de inicio de sesión en un terminal.
<Cuerpo texto>El hecho de que dos o más partes se identifiquen la una a la otra, se conoce como autenticación mutua. Un cliente puede autenticar a un servidor y este al cliente cuando surja la necesidad de establecer una sesión

segura entre los dos y emplear el cifrado. Esta autenticación asegura que el cliente no se está conectando sin darse cuenta y dando sus credenciales a un servidor no autorizado, que pueda usar y robar datos del servidor real.
En general, la autenticación mutua se implementa cuando los datos que se envían durante la sesión son de naturaleza confidencial, como historiales médicos o informes financieros.
<Nivel 2>Autenticación de factor múltiple
<Cuerpo texto>Cuando dos o más métodos de acceso se incluyen como parte del proceso, está implementando un sistema de autentificación múltiple. En la figura 5.2, puede observar los dos factores de autenticación. Este ejemplo requiere una tarjeta inteligente y un proceso de inicio de sesión y contraseña.
**********5_002.tif**********
<Pie figura>**Figura 5.2.** Autenticación de dos factores.
<Cuerpo texto>Un sistema de varios factores puede consistir en un sistema de dos factores, de tres, etc. Siempre que se incluya más de un factor en el proceso de autenticación, se considera un sistema de varios factores.
Por razones obvias, los factores que se empleen no deberían pertenecer a la misma categoría. Aunque incremente la dificultad para acceder al sistema requiriendo que los usuarios introduzcan dos combinaciones de usuario/contraseña, es mucho más recomendable combinar una sola combinación usuario/contraseña con un identificador biométrico u otra comprobación.
<Nivel 2>Seguridad operativa
<Cuerpo texto>La seguridad operativa se centra en cómo consigue sus objetivos una organización. También forma parte de la tríada de seguridad que incluye la seguridad física y de administración.
Como tal, las cuestiones de seguridad operativa incluyen NAC (*Network Access Control*, Control de acceso de red), autenticación y topologías de seguridad una vez que se ha completado la instalación de red. Entre ellas se encuentran las operaciones diarias de la red, las conexiones a otras redes, los planes de copias de seguridad y los de recuperación.
En resumen, la seguridad operativa abarca todo lo que no está relacionado con el diseño o la seguridad física de su red. En lugar de centrarse en los componentes físicos en los que se almacenan los datos, como el servidor, el énfasis recae ahora en la topología y las conexiones.
<Nota>**Nota:** Algunos vendedores utilizan el acrónico NAC para *Network Admission Control* (Control de admisión de red) en lugar del uso más aceptado, *Network Access Control*. Con independencia de cómo aparezca la palabra central del acrónimo, el concepto es el mismo.
<Cuerpo texto>Al principio, las cuestiones que gestione en el área operativa pueden resultar abrumadoras. Muchos de los ámbitos en los que se centrará son vulnerabilidades, debilidades o políticas de seguridad inadecuadas de los sistemas que utiliza. Por ejemplo, si implementa una política de expiración de contraseña completa, puede requerir a los usuarios que cambien sus contraseñas cada 30 o 60 días. Si el sistema no requiere rotación de contraseña (permite que se reutilicen las mismas contraseñas), tiene una vulnerabilidad que quizás no sea capaz de eliminar. Un usuario puede afrontar el movimiento de cambiar su contraseña limitándose a introducir el mismo valor y mantenerlo en uso.
Desde una perspectiva operativa, este tipo de sistema tiene debilidades en el cambio de contraseña. No hay nada que pueda hacer, aparte de instalar un proceso de inicio de sesión de alta seguridad o sustituir el sistema operativo. Sin embargo, no todas las soluciones son viables en términos de coste, tiempos de conversión y la posible negativa de una organización o sus socios ante la implementación de este cambio.
Esta dependencia de un sistema débil suele ser producto del hecho de que la mayoría de las compañías usan software de terceros para ahorrar costes o cumplir requerimientos de compatibilidad. Además, estos paquetes pueden requerir el uso de un sistema operativo específico. Si este sistema operativo tiene problemas de seguridad o vulnerabilidades significativas, sus obligaciones serán faraónicas porque seguirá siendo responsable de proporcionar seguridad en el entorno. Por ejemplo, su red corporativa segura nunca debería conectarse a Internet porque podría ser víctima de una serie interminable de posibles vulnerabilidades. Debe instalar soluciones de hardware y software para mejorar la seguridad y convencer a la administración de que estas medidas son más valiosas que el coste para implementarlas.
<Nivel 2>Tokens
<Cuerpo texto>Los *tokens* de seguridad son similares a los certificados. Contienen los derechos y los privilegios de acceso de los portadores como parte del *token*. Piense en los *tokens* como si se tratara de una pequeña pieza de datos que contiene una cantidad reducida de información sobre el usuario. No olvide que el término demandante se utiliza para el suscriptor de un proveedor de servicio de credenciales.
Muchos sistemas operativos generan un *token* que se aplica a todas las acciones que se llevan a cabo en el sistema informático. Si este elemento no le garantiza el acceso a cierta información, esta no se visualizará o se le denegará el acceso. El sistema de autenticación crea un *token* cada vez que un usuario se conecta o se inicia una sesión. Cuando concluye la sesión, este se destruye. La figura 5.3 muestra el proceso de *tokens* de seguridad.
**********5_003.tif**********
<Pie figura>**Figura 5.3.** Autenticación mediante token de seguridad.
<Nivel 2>Autenticación en potencia y problemas de acceso
<Cuerpo texto>Hay dos áreas problemáticas que debería conocer para el examen Security + porque se aplican a cuestiones de autenticación/acceso: el acceso transitivo y los ataques del lado del cliente. Ambos se explican a continuación.
<Nivel 3>Acceso transitivo
<Cuerpo texto>Relacionado con la transición, es necesario conocer este proceso para entender cómo se producen los problemas de acceso transitivo. Con este tipo de acceso, una parte (A) confía en otra (B). Si la segunda parte (B) se fía de una tercera (C), puede existir una relación en la que la primera parte (A) confíe en la tercera parte (C).
En los primeros sistemas operativos, se solía sacar partido de este proceso. En los actuales, como Windows Server 2008, los problemas con el acceso transitivo se solucionaron creando las confianzas transitivas, un tipo de relación que puede existir entre dominios (el antónimo es no transitivo). Cuando la relación de confianza es transitiva, la

relación entre la parte (A) y la parte (B) se transfiere como se describió más arriba (por ejemplo, A ahora confía en C). En todas las versiones de Active Directory, la opción predeterminada es que todos los dominios en una confianza de bosque tengan dos relaciones de confianza transitiva.
Aunque este proceso hace que la administración sea mucho más fácil cuando añade un nuevo dominio subordinado (no se requiere intervención administrativa para establecer las confianzas), deja abierta la posibilidad de que un *hacker* adquiera más confianza de la que debería uniéndose al dominio. En el ejercicio 5.1, aprenderá cómo validar la relación de confianza en Windows Server 2008, un importante paso para abordar este problema.
**********Inicio ejercicio**********
<Nivel 4>Ejercicio 5.1. Validar una relación de confianza
<Cuerpo texto>Como administrador, debería conocer qué relaciones de confianza existen entre los dominios. Para validar una relación de confianza en Windows Server 2008, siga estos pasos:
<Sep-med>1. Abra **Dominios y confianzas de Active Directory**.
2. Haga clic en su nombre de dominio y seleccione **Propiedades** en el menú.
3. Haga clic en la ficha **Confianzas** y seleccione el nombre del dominio o bosque que quiera validar.
4. Haga clic en **Propiedades**. Se abrirá el cuadro de diálogo para la confianza seleccionada.
5. Un poco más abajo del cuadro de diálogo, aparece el elemento **Transitividad de la confianza**. Haga clic en **Validar**.
6. Cuando aparezca el mensaje de confirmación, haga clic en **Aceptar**.
7. Salga de **Dominios y confianzas de Active Directory**.
**********Fin ejercicio**********
<Nivel 3>Ataques del lado del cliente
<Cuerpo texto>Un ataque del lado del cliente se dirige a las vulnerabilidades en las aplicaciones del cliente que interactúan con un servidor malicioso. De esta manera, un usuario accede al sitio de confianza (Web, FTP o casi cualquier otra aplicación) y descarga sin darse cuenta del código no autorizado (pensando que descarga música, vídeos, etc.). El código no autorizado permite al individuo malintencionado instalar o ejecutar programas en la máquina afectada de forma remota. Lo que es relevante para el tema de acceso es que los programas recién instalados se ejecutan con el nivel de privilegio del usuario que accede al servidor.
Si un usuario tiene privilegios elevados, por ejemplo, un administrador inexperto, el software malintencionado se ejecuta en ese nivel. En la mayoría de los casos, los programas que se ejecutan intentan llegar más allá del terminal en que se instalaron en un principio y encontrar su camino hasta el servidor/-es. A menudo, los datos a los que accede se suelen eliminar en Internet, usando HTTPS para cifrarlos y, así, reducir las posibilidades de que los detecten. HTTPS y HTTP Seguro se tratan en otro capítulo.
<Nivel 2>Cuestiones de autenticación a considerar
<Cuerpo texto>Puede establecer muchos parámetros y estándares diferentes para hacer que los miembros de su organización los cumplan. Para ello, es importante que considere las capacidades de las personas que están trabajando con estas políticas. Si está trabando en un entorno en el que las personas no son muy hábiles con la informática, puede que tenga que pasar mucho tiempo ayudándoles a recordar y recuperar contraseñas. Cada organización tiene sus propias particularidades y puede que sea necesario volver a evaluar sus directrices de seguridad cuando haya analizado al personal durante un período de tiempo y el gasto para implementar los sistemas de alta seguridad que se adapten a ellos. Recuerde que siempre es mejor educar a los usuarios (sensibilizarlos) que reducir la seguridad.
Establecer la seguridad de autenticación, sobre todo para respaldar a los usuarios, puede convertirse en una tarea de mantenimiento muy elevada para los administradores de red. Por un lado, requiere que los miembros puedan autentificarse de forma sencilla. Por otro, que se establezca una seguridad que proteja los recursos de la compañía. A continuación, encontrará algunas pautas para facilitar este proceso:
<Sep-med>* **No se fíe de nombres populares y tendencias actuales que hacen que una contraseña sea predecible:** Por ejemplo, cada mes de enero, los equipos de la Super Bowl se convierte en contraseñas probables, al igual que las variaciones con los nombres y números de los jugadores. Esto puede crear un problema de seguridad para los centros informáticos.
* **Utilice pruebas de identidad siempre que surjan problemas entre identificación y autenticación:** El proceso de identificación comienza cuando un ID de usuario o nombre de inicio de sesión se escribe en una pantalla de acceso. La autenticación se consigue desafiando la petición de alguien que va a acceder a los recursos.
* **Incorporar un segundo valor, como el apellido de soltera de su madre, para comprobar la identidad de un usuario:** Esto es útil cuando se recurre a la prueba de identificación porque una persona reclame ser el usuario pero no pueda autentificarse, por ejemplo, porque ha perdido su contraseña.
**********INICIO DE NOTA**********
<Nivel 3>Autenticación con varios factores y seguridad
<Nota>El CEO (*Chief Executive Officer*, Director ejecutivo) está cada vez más preocupadopor la seguridad informática y la laxitud de los usuarios. Se ha dado cuenta de que éstos suelen irse de la oficina al final de la jornada sin desconectar sus cuentas. La compañía está intentando conseguir un contrato que está relacionado con el gobierno y requerirá medidas de seguridad adicionales. ¿Qué les sugeriría?
Antes que nada, debería recomendar a la empresa implementar un sistema de autenticación de varios factores, que consistiría en una tarjeta inteligente y un proceso de nombre de usuario/contraseña. La mayoría de los lectores de tarjetas inteligentes pueden configurarse para requerir que la tarjeta permanezca insertada en el lector todo el tiempo que el usuario esté conectado. Si la tarjeta se extrae, por ejemplo, al final de la jornada, el terminal desconectará de forma automática al usuario. Requiriendo un proceso nombre de usuario/contraseña, puede seguir proporcionando seguridad aunque roben la tarjeta inteligente. Esta solución proporciona una seguridad razonable y no incrementa demasiado los costes.

Otras sugerencias son considerar controles de acceso adicionales, como alarmas de perímetro y controles de acceso físico a áreas confidenciales. Es probable que el gobierno requiera todo esto, aunque estas medidas no obligarán a los usuarios a desconectar las sesiones cuando dejen los terminales.
**********FIN DE NOTA**********
<Cuerpo texto>Un problema inherente a muchas implementaciones para probar la identidad es que son preguntas que otra persona podría adivinar con facilidad o aprender su valor (¿De qué color son sus ojos?). Para aumentar la dificultad de que alguien pueda aportar pruebas fraudulentas, solo debería utilizar preguntas que sean más difíciles de adivinar o introducir biometría como identificación de voz. Bajo ningún concepto debería permitir acceso inmediato a la persona que prueba su identidad. En su lugar, la información de acceso tendría que enviarse a la cuenta de correo electrónico de su registro.
<Nivel 1>Conectividad de acceso remoto
<Cuerpo texto>Uno de los principales propósitos de tener una red es la habilidad de conectar sistemas. Cuando las redes han ido creciendo, muchas tecnologías han aparecido en escena para hacer que este proceso sea más fácil y seguro. Un área clave de preocupación está relacionada con la conexión de sistemas y otras redes que no forman parte de su red. Las siguientes secciones describen los protocolos más comunes para facilitar la conectividad remota entre sistemas.
**********INICIO DE NOTA**********
<Nivel 3>Historia antigua: protocolo de Internet para líneas en serie
<Nota>SLIP (*Serial Line Internet Protocol*, Protocolo de Internet para líneas en serie) es un protocolo antiguo que se utilizaba en los inicios de los entornos de acceso remoto y servía como punto de inicio para la mayoría de comunicaciones remotas. En su origen, SLIP se diseñó para conectarse a sistemas Unix en un entorno de marcado y solo admitía comunicaciones en serie.
Era un protocolo muy simple. Solo podía emplearse para pasar tráfico a través de TCP/IP y ni era seguro ni eficiente. Aunque algunos sistemas siguen siendo compatibles con SLIP, hoy en día se utiliza únicamente para sistema de legado y debería evitarse en la medida de lo posible.
**********FIN DE NOTA**********
<Nota>**Nota:** Cualquier autenticación realizada por un usuario remoto se conoce como autenticación remota. En general, esta se lleva a cabo usando TACACS (*Terminal Access Controller Access Control System*, Sistema de control de acceso mediante control del acceso desde terminales) o RADIUS (*Remote Authentication Dial In User Service*, Servicio de autenticación remota telefónica de usuario).
<Nivel 2>Protocolo punto a punto
<Cuerpo texto>Publicado en 1994, PPP (*Point-to-Point Protocol*, Protocolo punto a punto) presta soporte a muchos protocolos, entre los que se incluyen AppleTalk, IPX (*Internetwork Packet Exchange*, Intercambio de paquetes inter red) y DECnet (grupo de productos de Comunicaciones, desarrollado por la firma Digital Equipment Corporation). PPP funciona con POTS (*Plain Old Telephone Service*, Servicio telefónico ordinario antiguo), ISDN (*Integrated Services Digital Network*, Red digital de servicios integrados) y otras conexiones más rápidas como T1. PPP no proporciona seguridad de datos, pero sí autenticación mediante el protocolo CHAP (*Challenge Handshake Authentication Protocol*, Protocolo de autenticación por desafío mutuo).
La figura 5.4 muestra una conexión PPP sobre una línea ISDN. En caso de ISDN, PPP emplearía un canal 64 Kbps B para la transmisión. PPP permite que se conecten o vinculen muchos canales en una conexión de red (por ejemplo, ISDN) para formar una única conexión virtual.
**********5_004.tif**********
<Pie figura>**Figura 5.4.** PPP usando un único canal B en una conexión ISDN.
<Cuerpo texto>PPP funciona encapsulando el tráfico de red en un protocolo llamado NCP (*Network Control Protocol*, Protocolo de control de red). La autenticación la gestiona LCP (*Link Control Protocol*, Protocolo de control de enlace). Una conexión PPP permite a los usuarios remotos iniciar sesión en la red y tener acceso como si se tratara de usuarios locales. Tenga en cuenta que PPP no proporciona servicios de cifrado para el canal.
Como ya habrá adivinado, la naturaleza insegura de PPP la hace muy poco apropiada para conexiones WAN. Para solventar esta cuestión, se han creado otros protocolos que sacan partido a la flexibilidad de PPP y se basan en él. Compruebe que todas sus conexiones PPP utilizan canales seguros, conexiones específicas o de alta velocidad.
Los usuarios remotos que se conectan directamente a un sistema no tienen por qué tener habilitadas capacidades de cifrado. Si la conexión es directa, la posibilidad de que alguien pueda pinchar una línea de teléfono es bastante reducida. Sin embargo, debería asegurarse de que todas las conexiones de una red emplean un sistema orientado al tunelado.
<Nivel 2>Trabajar con protocolos de túnel
<Cuerpo texto>Los protocolos de túnel añaden una propiedad a la red: la habilidad de crear túneles entre redes que puede hacerlas más seguras, admitir protocolos adicionales y proporcionar rutas virtuales entre sistemas. La mejor forma de pensar en el tunelado es imaginar datos confidenciales que se encapsulan en otros paquetes que se envían a través de la red pública. Una vez que se han recibido en el otro extremo, la información confidencial se extrae de los paquetes y se devuelve a su estado original.
Los protocolos más comunes que se utilizan para el tunelado son los siguientes:
<Sep-med>* **PPTP (*Point-to-Point Tunneling*, Protocolo de túnel punto a punto):** Admite la encapsulación en un entorno único punto a punto. PPTP encapsula y cifra los paquetes PPP. Esto hace que PPTP sea el protocolo favorito de nivel inferior para las redes. La negociación entre los dos extremos de una conexión PPTP se lleva a cabo de forma segura y, cuando esta concluye, el canal se cifra. Esta es una de las mayores debilidades de PPTP. Así, un dispositivo de captura de paquetes, como un analizador de protocolos *sniffer*, que recoge el proceso de negociación, podría utilizar esa información con el fin de determinar el tipo de conexión e información sobre el funcionamiento del

túnel. Microsoft desarrolló PPTP y este es compatible con la mayoría de los productos de la compañía. PPTP usa el puerto 1723 y TCP para las conexiones.

* **L2F (*Layer 2 Forwarding*, Reenvío Capa 2):** Cisco creó este protocolo como método para crear túneles, sobre todo, en conexiones de marcado. En términos de capacidad, es similar a PPP y no debería utilizarse en redes WAN. Proporciona autenticación pero no cifrado. L2F usa el puerto 1701 y TCP para las conexiones.
* **L2TP (*Layer 2 Tunneling Protocol*, Protocolo de túnel Capa 2):** Microsoft y Cisco llegaron a un acuerdo para combinar sus respectivos protocolos de túnel en uno solo: L2TP. Se trata de un híbrido de PPTP y L2F. En esencia, es un protocolo punto a punto, compatible con muchos protocolos de red y puede emplearse para otras redes que no sean TCP/IP. L2TP funciona sobre IPX (*Internetwork Packet Exchange*, Intercambio de paquetes inter red), SNA (*Systems Network Architecture*, Arquitectura de sistemas de red) e IP (*Internet Protocol*, Protocolo de Internet), de modo que puede emplearse como puente para muchos tipos de sistemas. Su principal problema es que no proporciona seguridad de datos, la información no está cifrada. No obstante, la seguridad la pueden proporcionar protocolos como IPSec. L2TP usa el puerto 1701 y UDP para las conexiones.
* **SSH (*Secure Shell*, Protocolo de shell seguro):** Protocolo de túnel diseñado en su origen para sistemas Unix. Emplea el cifrado para establecer una conexión segura entre dos sistemas. SSH también proporciona programas de seguridad equivalente para estándares como Telnet (*Telecommunication Network*, Red de telecomunicaciones), FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos) y muchas otras aplicaciones orientadas a las comunicaciones. Además, SSH también está disponible para sistemas Windows, lo que le convierte en el método favorito de seguridad para Telnet y otros programas de texto no cifrado en entornos Unix. SSH utiliza el puerto 22 y TCP para las conexiones.
* **IPSec (*Internet Protocol Security*, Seguridad del Protocolo de Internet):** No es un protocolo de túnel pero se utiliza en combinación con protocolos de tunelado. Está orientado sobre todo hacia conexiones LAN a LAN, pero también puede emplearse para conexiones remotas. Proporciona autenticación y cifrado seguros de los datos y encabezados, lo cual hace que se trate de una buena elección en términos de seguridad. IPSec puede funcionar en modo túnel o transporte. En el primero, se cifran los datos o la carga, y los encabezados de los mensajes. En modo transporte, solo se cifra la carga. IPSec es un complemento para IPv4 y se basa en IPv6.

<Nivel 2>Trabajar con RADIUS

<Cuerpo texto>RADIUS (*Remote Authentication Dial In User Service*, Servicio de autenticación remota telefónica de usuario) es un mecanismo que permite la autenticación de conexiones remotas y otras redes. En principio, se ideó para conexiones de marcado, pero ha evolucionado mucho y tiene múltiples características modernas. Se tra de un estándar de IETF (*Internet Engineering Task Force*, Grupo especial sobre ingeniería de Internet) y lo han implementado la mayoría de los principales fabricantes de sistemas operativos.

Un servidor RADIUS puede gestionarse de forma central y los servidores que permiten acceso a la red pueden verificar con él si una llamada entrante está autorizada. En una red compleja con muchas conexiones, conlleva que un solo servidor realice todas las autenticaciones.

La figura 5.5 es un ejemplo de servidor RADIUS comunicándose con un ISP (*Internet Service Provider*, Proveedor de servicios de Internet) para permitir el acceso a un usuario remoto. Tenga en cuenta que el servidor remoto está funcionando como cliente del servidor RADIUS. Esto permite una administración centralizada de los derechos de acceso.

**********5_005.tif**********

<Pie figura>**Figura 5.5.** El cliente RADIUS gestiona la conexión local y la autentifica frente al servidor central.

<Cuerpo texto>Utilice RADIUS cuando quiera mejorar la seguridad de red e implementar un único servicio con el fin de que autentique a los usuarios que se conecten de forma remota a la red. Con esto, tendrá una única fuente que lleve a cabo la autenticación. De forma adicional, puede implementar auditorías y responsabilidad en el servidor RADIUS.

La mayor dificultad con un entorno de un único servidor RADIUS es que toda la red puede rechazar las conexiones si el servidor no funciona bien. Por este motivo, muchos sistemas RADIUS permiten que se utilicen varios servidores para incrementar la fiabilidad. Todos estos servidores son componentes esenciales de la infraestructura y deben estar protegidos ante los ataques.

<Nivel 2>TACACS/TACACS+/XTACACS

<Cuerpo texto>TACACS (*Terminal Access Controller Access-Control System*, Sistema de control de acceso mediante control del acceso desde terminales) es un entorno orientado a cliente-servidor y funciona de forma similar a RADIUS. XTACACS (*Extended TACACS*, TACACS ampliado) sustituye al original y combina la autenticación y la autorización con el inicio de sesión para habilitar auditorías.

El método más actual o nivel de TACACS es TACACS+, que sustituye a las dos versiones anteriores. TACACS+ permite que se acepten credenciales de varios métodos, incluyendo Kerberos. El proceso TACACS cliente/servidor se produce del mismo modo que el proceso RADIUS que observó en la figura 5.5.

Cisco ha implementado TACACS+ de forma generalizada como alternativa para las conexiones. Se espera que este acabe siendo tan aceptado como RADIUS.

<Nota>**Truco:** Recuerde, RADIUS y TACACS pueden emplearse para autenticar las conexiones.

<Nivel 2>Administración VLAN

<Cuerpo texto>Una VLAN (*Virtual Local Area Network*, Red de área local virtual) le permite crear grupos de usuarios y sistemas, así como segmentarlos en la red, lo cual le permite ocultar segmentos de la red de otros segmentos y, de ese modo, controlar el acceso. También puede establecer redes VLAN para controlar las rutas que toman los datos para ir de un sitio a otro. Una VLAN es una buena manera de contener el tráfico de red a cierta área de red.

<Nota>**Truco:** Piense en una VLAN como una red de host que actúa como si estuvieran conectados a través de cableado físico, aunque no exista tal conexión entre ellos.
<Cuerpo texto>En una LAN, los host pueden comunicarse entre sí utilizando las difusiones y no necesitan dispositivos de reenvío, como enrutadores. Cuando la LAN crezca, también se incrementará el número de difusiones. En cambio, si se reduce su tamaño segmentándola en grupos pequeños (VLAN) disminuye el tamaño de los dominios de difusión. Las ventajas que consigue con ello son reducir el alcance de las difusiones, mejorando el rendimiento y la manejabilidad, así como disminuir la dependencia en la topología física. No obstante, desde el punto de vista de este examen, el principal beneficio es que las redes VLAN pueden incrementar la seguridad permitiendo a los usuarios con niveles similares de confidencialidad de datos que se segmenten juntas.
La figura 5.6 ilustra la creación de tres redes VLAN en una única red.
**********5_006.tif**********
<Pie figura>**Figura 5.6.** Típica red VLAN segmentada.
<Nivel 1>Servicios de autenticación
<Cuerpo texto>Los servicios de autenticación son la implementación de la tecnología en cuestión. Para esta parte del temario del examen, el énfasis recae en LDAP (*Lightweight Directory Access Protocol*, Protocolo ligero de acceso a directorios) y Kerberos, aunque existan muchas otras posibilidades como IAS (*Internet Authentication Service*, Servicio de autentificación de Internet) y CAS (*Central Authentication Service*, Servicio de autenticación central), que están fuera del ámbito de este examen. Las iniciativas de inicio de sesión únicas completan la explicación de este apartado.
<Nivel 2>LDAP
<Cuerpo texto>LDAP (*Lightweight Directory Access Protocol*, Protocolo ligero de acceso a directorios) es un protocolo de acceso a directorio estandarizado que permite que se realicen consultas de directorios (en concreto, directorios reducidos basados en X.500).
Si un servicio de directorio mantiene el LDAP, puede consultar el directorio con un cliente LDAP. Por otro lado, la popularidad de este protocolo está incrementando y empezando a utilizarse de forma generalizada en páginas *on-line* blancas y amarillas.
LDAP es el principal protocolo de acceso utilizado por Active Directory. De forma predeterminada, opera en el puerto 389. La sintaxis LDAP usa comas entre nombres.
<Nivel 2>Kerberos
<Cuerpo texto>Kerberos es un protocolo de autenticación que recibe su nombre del mítico perro de tres cabezas que guardaba las puertas del inframundo. Creado por MIT, Kerberos es muy popular como método de autenticación ya que permite un único inicio de sesión para una red distribuida.
La autenticación Kerberos usa un KDC (*Key Distribution Center*, Centro de distribución de claves) para dirigir el proceso. El KDC autentica el principal (que puede ser un usuario, un programa o un sistema) y le proporciona un ticket. Cuando este se expide, puede emplearse para autenticarse frente a otros principales. Esto ocurre de forma automática si otro principal ejecuta una solicitud o servicio.
Kerberos se está convirtiendo en un estándar común en los entornos de red. Su principal debilidad es que KDC puede ser un único punto de fallo. Si este se bloquea, el proceso de autenticación se detendrá. La figura 5.7 ilustra el proceso de autenticación de Kerberos y cómo se presenta el ticket a los sistemas autorizados por el KDC.
**********5_007.tif**********
<Pie figura>**Figura 5.7.** Proceso de autenticación de Kerberos.
<Nivel 2>Iniciativas de inicio de sesión único
<Cuerpo texto>Uno de los mayores problemas que deben afrontar los sistemas más grandes es la necesidad de que los usuarios accedan a varios sistemas o aplicaciones. El propósito de una SSO (*Single Sign-On*, Inicio de sesión único) es proporcionar acceso a los usuarios a todas las aplicaciones y sistemas que necesiten cuando inicien sesión. Esto se está convirtiendo en una realidad en muchos entornos, incluyendo Kerberos, Microsoft Active Directory, Novell eDirectory y algunas implementaciones de modelo de certificados.
<Nota>**Nota:** El inicio de sesión único es una bendición y una maldición al mismo tiempo. Por un lado, es positivo porque una vez que el usuario se ha autenticado, puede acceder a todos los recursos de la red y navegar por varios directorios. Por otro lado, es negativo porque elimina puertas que, de lo contrario, existirían entre el usuario y varios recursos.
<Cuerpo texto>En el caso de Kerberos, un único *token* permite a todas las aplicaciones que lo utilizan aceptar un usuario como válido. Lo importante es recordar que en este proceso todas aquellas aplicaciones que quieran utilizar SSO deben aceptar y procesar el *token* presentado por Kerberos.
El AD (*Active Directory*, Directorio activo) funciona de una manera algo diferente. Un servidor que ejecuta AD retiene información sobre todos los derechos de acceso de los usuarios y grupos de la red. Cuando un usuario inicia sesión en el sistema, AD le expide un GUID (*Globally Unique Identifier*, Identificador único global). Las aplicaciones que admite AD pueden usar este GUID con el fin de proporcionar control de acceso. La figura 5.8 ilustra este proceso con más detalle. En este ejemplo, la aplicación de la base de datos, el cliente de correo electrónico y las impresoras autentican con el mismo inicio de sesión. Al igual que Kerberos, este proceso requiere que todas las aplicaciones que desean sacar partido del AD acepten sus controles y las directrices
De este modo, el usuario no tiene que tener un inicio de sesión independiente, correo electrónico, ni contraseñas de las aplicaciones. Usar AD simplifica el proceso de inicio de sesión para los usuarios y reduce los requerimientos de soporte técnico para los administradores. El acceso puede establecerse a través de grupos e imponerse mediante la pertenencia a grupos.
**********5_008.tif**********
<Pie figura>**Figura 5.8.** AD validando usuario.

<Cuerpo texto>En una red descentralizada, las contraseñas SSO se almacenan en cada servidor y pueden representar un riesgo de seguridad. Es importante imponer los cambios de contraseña y hacer que algunas se actualicen en la organización con cierta regularidad.
<Nota>**Nota:** Aunque un inicio de sesión único no es lo opuesto a la autenticación de varios factores, se suele pensar que sí. El factor uno, dos y tres de autenticación solo se refiere al número de elementos que un usuario debe proporcionar para autenticarse. Esta puede basarse en algo que tenga (una tarjeta inteligente), algo que sabe (una contraseña) o algo único (biometría), entre otros ejemplos. Cuando se haya realizado la autenticación, todavía puede aplicarse el inicio de sesión único durante la sesión del usuario.
<Nivel 1>Control de acceso
<Cuerpo texto>Los tres métodos de control de acceso principales son los siguientes:
<Sep-med>* **MAC (*Mandatory Access Control*, Control de acceso obligatorio):** Todo el acceso está predefinido.
* **DAC (*Discretionary Access Control*, Control de acceso discrecional):** Incorpora alguna flexibilidad.
* **RBAC (*Role-Based Access Control*, Control de acceso basado en roles):** Permite al rol del usuario dictar las capacidades de acceso.
<Cuerpo texto>Un cuarto método, que también utiliza el acrónimo RBAC (*Rule-Based Access Control*, Control de acceso basado en reglas), está adquiriendo popularidad. Cada uno de ellos tiene ventajas y desventajas para la organización, desde el punto de vista de la seguridad.
El método que elija se verá influenciado de forma significativa por las convicciones de su organización y sobre cómo necesitan compartir la información. En un entorno de alta seguridad, la tendencia sería implementar un método MAC o RBAC. En el contexto de una empresa tradicional o una escuela, lo habitual sería aplicar un método DAC. Debería realizar algunas consultas en la organización para entender cómo un departamento en particular y la compañía en general quieren introducir los modelos de control de acceso. Con ello, se recopilará opiniones de todas las partes involucradas, lo cual le servirá para conocer las directrices básicas que quiere establecer y cómo deberían implementarse.
En las siguientes secciones, nos centraremos en cada uno de estos métodos desde una perspectiva empresarial.
<Nivel 2>Control de acceso obligatorio
<Cuerpo texto>MAC es, sin duda alguna, un método rígido para permitir el acceso a la información. En un entorno MAC, todas las capacidades de acceso están predefinidas. Los usuarios no pueden compartir información a menos que los administradores hayan establecido estos derechos. Son precisamente los administradores los que deben llevar a cabo cualquier cambio que sea necesario, ya que este proceso impone un modelo rígido de seguridad.
Para que un modelo MAC funcione de forma efectiva, los administradores y los diseñadores de red deben pensar en las relaciones con cautela. La ventaja de este modelo es que el acceso de seguridad está bien establecido y definido, haciendo que las infracciones de seguridad sean más fáciles de investigar y corregir. Un modelo MAC bien diseñado puede hacer que la tarea de controlar la información sea más fácil y bloquear la red de forma básica. Las mayores desventajas son la falta de flexibilidad y el hecho de que necesita cambiar con el tiempo. La falta de habilidad del personal para gestionar estos cambios puede provocar que este modelo sea difícil de mantener en ocasiones.
MAC se utiliza en entornos donde la confidencialidad es una fuerza mayor. A menudo, emplea clasificaciones gubernamentales y militares (etiquetas) como Confidencial.
<Nivel 2> Control de acceso discrecional
<Cuerpo texto>En el modelo DAC, los usuarios de red tienen alguna flexibilidad en lo que respecta a cómo acceder a la información. Además, les permite compartir de forma dinámica la información con otros usuarios. Por otro lado, aunque conlleve un entorno más flexible, aumenta los riesgos de revelación de información. Por ello, los administradores tendrán más dificultades a la hora de asegurar que el acceso a la información está controlado y solo se han concedido los accesos adecuados.
Un ejemplo clásico de DAC es la estructura de permisos que existe para terceros con archivos en el entorno Unix/Linux. Todos los permisos del sistema operativo se clasifican en tres grupos de usuarios: propietario, grupo y otros. Los permisos asociados con el propietario y el grupo al que este pertenece se basan en sus roles, pero todos aquellos que no son el propietario o miembro del grupo de propietarios, pertenecen a la categoría de otros.
Los permisos de este último se establecen de forma independiente de los otros dos y, exceptuando casos especiales, son una combinación de lectura, escritura y ejecución. Dentro de este entorno, puede crear una base de datos y darse permiso (propietario) para leer y escribir, dar a otros administradores (grupo) solo permiso para leer y no dar permiso a los que no estén en el grupo administradores (otros).
Podría ser tan fácil como crear un archivo de *script* que limpia los archivos de inicio de sesión y libera espacio en el terminal. Así, podría darse acceso a sí mismo(propietario) a todos los derechos, dar a otros administradores (grupo) la habilidad de leer y ejecutar, y dar a los usuarios básicos (otros) solo el derecho a ejecutar.
<Nivel 2>Control de acceso basado en roles
<Cuerpo texto>El modelo RBAC se centra en el control de acceso basándose en los roles establecidos en una organización. Este tipo de modelo implementa el acceso por función profesional o por responsabilidad. Así, dependiendo de si el empleado tiene uno o más roles, se le permitirá acceso a una determinada información. Si una persona cambia de rol, ya no estará disponible el rol anterior. El modelo RBAC proporcionan más flexibilidad que el MAC y menos que el DAC. Sin embargo, tiene la ventaja de basarse estrictamente en funciones profesionales, frente a las necesidades de un individuo.
En lugar de pensar "Denise necesita editar archivos", RBAC recurre a la lógica: "Los redactores necesitan editar archivos" y "Denise es miembro del grupo redactores". Este modelo siempre es bueno para utilizarlo en un entorno en el que haya un tránsito elevado de empleados.
<Nivel 2>Control de acceso basado en reglas

<Cuerpo texto>RBAC (*Rule-Based Access Control*, Control de acceso basado en reglas) utiliza la configuración de políticas de seguridad establecidas con anterioridad para tomar todas las decisiones. Estas reglas pueden denegar a todos salvo a los que aparezcan en una lista de forma específica (una lista de admitidos) o denegar solo a los que aparecen en la lista de forma específica (verdadera lista de denegación). Las entradas de la lista pueden ser nombres de usuarios reales, direcciones IP, nombres de host o incluso dominios. Los modelos basados en reglas suelen emplearse en combinación con los que se basan el roles para añadir mayor flexibilidad.
La forma más fácil de implementar RBAC es con ACL (*Access Control Lists*, Listas de control de acceso) que se trata más adelante. Las listas ACL crean las reglas por las que se rige el modelo de control de acceso.
<Nivel 1>Implementar las prácticas recomendadas de control de acceso
<Cuerpo texto>El modo de implementar el control de acceso marca la diferencia en términos de seguridad. En esta sección, analizaremos las tarjetas inteligentes, las listas de control de acceso, los sistemas operativos de confianza y la configuración de los enrutadores seguros.
<Nivel 2>Tarjetas inteligentes
<Cuerpo texto>En general, las tarjetas inteligentes se utilizan para control de acceso y seguridad. La tarjeta suele contener una pequeña memoria que puede emplear para almacenar información de acceso y permisos.
Estas tarjetas son difíciles de falsificar pero fáciles de robar. Si alguien se hace con una, tendrá todos los accesos que permite la tarjeta. Para evitarlo, muchas organizaciones no ponen marcas identificativas en sus tarjetas inteligentes con el fin de que sea más difícil que alguien las utilice.
Para añadir seguridad, se requiere una clave o contraseña para activar muchas tarjetas inteligentes modernas y se emplea un cifrado para proteger su contenido. En algunos casos, si introduce la clave errónea varias veces (tres por lo general), la tarjeta se bloqueará. De esta maneramejora más aún la seguridad.
Muchos países europeos están empezando a utilizar tarjetas inteligentes en lugar de tarjetas de crédito de tira magnética porque ofrecen seguridad adicional y pueden contener más información.
<Nota>**Truco:** Cuando piense en una tarjeta inteligente, no olvide que esta herramienta puede emplearse tanto para la autenticación como para el almacenamiento. La tarjeta no solo le identifica, también guarda información relevante. Por ejemplo, imagine una tarjeta de débito con la que actualiza el balance de gastos de su cuenta bancaria en lugar de una tarjeta de crédito que solo contiene su número de cuenta y se limitará a cargar los gastos en ella con posterioridad.
**********INICIO DE NOTA**********
<Nivel 3>Trabajar con tarjetas inteligentes
<Listados>Le han pedido que colabore en la resolución de un problema que se está produciendo en el laboratorio informático de su universidad. Los estudiantes se están quejando de que hay un virus que están infectando unidades *flash* que llevan allí. ¿Cómo puede ayudarles a remediar esta situación?
Debería asegurarse de que todos los sistemas del laboratorio de la facultad tienen software antivirus y de que está actualizado. Con ello evitará que virus conocidos entren en el sistema de la universidad y se transfieran a los archivos de los estudiantes. También puede evaluar si estos ordenadores deberían tener medios extraíbles instalados. Muchos fabricantes venden sistemas llamados clientes básicos que no proporcionan ningún disco de almacenamiento o medio extraíble en sus terminales. Los clientes básicos utilizan servidores específicos para descargar aplicaciones, datos y cualquier otro tipo de información que necesiten ejecutar. Esto elimina el peligro de que se introduzcan virus en los discos de los estudiantes.
**********FIN DE NOTA**********
<Cuerpo texto>Principalmente, hay dos tipos de tarjetas inteligentes, que trataremos en las siguientes secciones.
<Nivel 3>Tarjeta de acceso común
<Cuerpo texto>Un tipo de tarjeta es la CAC (*Common Access Card*, Tarjeta de acceso común). Estas tarjetas las expide el Departamento de Defensa como tarjeta de identificación/autenticación general para personal militar, contratistas y empleados que no forman parte del departamento. Aparece una imagen en la parte frontal de la tarjeta con un chip integrado debajo y un código de barras. En la parte trasera de la tarjeta, hay una tira magnética y otro código de barras.
La CAC se utiliza para acceder a ordenadores del Departamento de Defensa, abrir el correo electrónico e implementar PKI (*Public Key Infrastructure*, Infraestructura de clave pública). En 2008, el año más reciente del que hay estadísticas disponibles, se expidieron unos 17 millones de tarjetas. Puede encontrar información actualizada sobre las tarjetas CAC en http://www.cac.mil.
<Nivel 3>Verificación de identificación personal
<Cuerpo texto>Lo que CAC es para los empleados militares, PIV (*Personal Identification Verification*, Verificación de identificación personal) es para los empleados federales y sus contratistas. Por la HSPD-12 (*Homeland Security Presidential Directive number 12*, Directiva presidencial de seguridad nacional número 12), el PIV acabará siendo un requisito para todos los empleados del gobierno estadounidense y sus contratistas. Será necesario para obtener acceso (físico y lógico) a los recursos del gobierno.
<Nivel 2>Listas de control de acceso
<Cuerpo texto>Las ACL (*Access Control Lists*, Listas de control de acceso) habilita los dispositivos de su red para ignorar peticiones de usuarios o sistemas específicos, o para garantizarles ciertas capacidades de red. Puede darse el caso de que una dirección IP esté escaneando continuamente su red y puede bloquearla. Si la bloquea en el enrutador, la dirección IP será rechazada de forma automática cada vez que intente utilizar su red.
Las listas ACL permiten que se establezca un grupo de controles de acceso más rígido en su red. El proceso básico de control permite al administrador que diseñe y adapte la red para gestionar amenazas de seguridad específicas. Las siguientes secciones se centran en los enfoques de ACL, incluyendo la denegación implícita y las reglas de cortafuegos.

<Nivel 3>Denegación implícita
<Cuerpo texto>En las listas ACL existe una condición conocida como denegación implícita, Que se incluye al final de estas. Esto quiere decir que si la condición que se trata no se ha garantizado explícitamente, se deniega. La mejor forma de entenderlo es utilizar una analogía: imagine que va a celebrar una fiesta y ha hecho una lista de invitados. Además, tiene un "gorila" en la puerta. Cuando van llegando los clientes, este comprueba la lista de invitados. Si el nombre no aparece en la lista, se les deniega la entrada. No tiene que comunicarle que no deje entrar a Evan, Kristin o Spencer porque sus nombres no aparecen en la lista y, por tanto, se les deniega el acceso de forma implícita.
Se mantiene el mismo principio en ACL. La entidad a la que se le deniega el acceso porque no aparece en la lista puede ser una dirección de origen, de destino, un tipo de paquete o casi cualquier cosa a la que quiera denegar el acceso.
<Nivel 3>Reglas de cortafuegos
<Cuerpo texto>Las reglas de cortafuegos actúan como las listas ACL y se utilizan para determinar qué tráfico puede pasar entre el cortafuegos y la red interna. Hay tres posibles acciones que puede llevar a cabo basándose en los criterios de las reglas:
<Sep-med>* Bloquear la conexión.
* Permitir la conexión.
* Permitir la conexión solo si es segura.
<Cuerpo texto>Las reglas pueden aplicarse al tráfico de entrada o de salida, y a cualquier tipo de red (LAN, inalámbrica, BPN o acceso remoto). Con cierta regularidad, debería realizar auditorías en las reglas del cortafuegos y verificar que está obteniendo los resultados que desea o realizar las modificaciones necesarias.
<Nivel 2>Sistema operativo de confianza
<Cuerpo texto>Un TOS (*Trusted Operating System*, Sistema operativo de confianza) es cualquier sistema operativo que cumpla los requisitos de seguridad exigidos por el gobierno. El grupo de estándares más utilizados para la seguridad es CC (*Common Criteria*, Criterios comunes). Este documento es una suma de esfuerzos procedentes de Canadá, Francia, Alemania, Holanda, Reino Unido y Estados Unidos. Los estándares resumen un grupo de criterios de evaluación flexible, divididos en siete EAL (*Evaluation Assurance Levels*, Niveles de confianza en la evaluación). A continuación, se describen con brevedad los siete niveles:
<Nota>**Nota:** Cuando se estaba escribiendo este libro, la última versión del estándar era 3.1 y estaba disponible en http://www.commoncriteriaportal.org. El sitio Web también mantiene un registro de productos certificados por CC.
<Sep-med>* **EAL 1:** Se utiliza principalmente cuando el usuario quiere asegurarse de que el sistema funciona de forma correcta y que las amenazas de seguridad no se consideran serias.
* **EAL 2:** Requiere que los desarrolladores de los productos empleen las prácticas de diseño recomendadas. La seguridad no se considera una prioridad esencial en la certificación EAL.
* **EAL 3:** Necesita serios esfuerzos de desarrollo para proporcionar niveles de seguridad moderados.
* **EAL 4:** Requiere una ingeniería de seguridad positiva basándose en las prácticas recomendadas de desarrollo comercial. Está previsto que EAL 4 se convierta en el punto de referencia común para los sistemas comerciales.
* **EAL 5:** Su propósito es asegurar que la ingeniería de seguridad se implemente en un producto desde las fases iniciales de diseño. Está previsto para asegurar niveles de seguridad elevados. La documentación EAL indica que, con toda probabilidad, se requerirán consideraciones de diseño especiales para adquirir este nivel de certificación.
* **EAL 6:** Ofrece un gran nivel de confianza en la ingeniería de seguridad especializada. Esta certificación indica altos niveles de protección frente a riesgos significativos. Los sistemas con certificación EAL 6 serán muy seguros ante la invasión de posibles ataques.
* **EAL 7:** Está diseñado para niveles de seguridad muy elevados. La certificación requiere una comprobación exhaustiva, mediciones y revisiones completas de cada componente individual.
<Cuerpo texto>La certificación EAL ha sustituido al sistema de certificaciones TCSEC (*Trusted Computer Systems Evaluation Criteria*, Criterios de evaluación de sistemas informáticos de confianza), que eran más populares en EE. UU. También han remplazado a ITSEC (*Information Technology Security Evaluation Criteria*, Criterios de evaluación de seguridad en tecnologías de la información) que era más conocido en Europa. El nivel de certificación recomendado para los sistemas comerciales es el EAL 4.
Hoy en día, solo algunos sistemas operativos han obtenido el nivel EAL 4 y, por muy recto que pueda ser un sistema, no significa que su implementación individual esté funcionando en ese nivel. Si este no utiliza las medidas de seguridad disponibles, está funcionando por debajo de lo requerido.
**********INICIO DE NOTA**********
<Nivel 3>Implementar un entorno de servidor seguro
<Nota>Imagine que forma parte del equipo que tomará la decisión de comprar un nuevo servidor para su organización, el cual tendrá que ser relativamente seguro y apropiado para almacenar información confidencial. También será parte de un entorno de comercio electrónico. ¿Cómo puede asesorar al equipo?
Puede ser muy útil para que el sistema operativo esté certificado por los criterios comunes. Puede visitar el sitio Web http://www.commoncriteriaportal.org/products/?expand#OS para identificar qué sistemas y productos están certificados por EAL 4. Anime a los miembros del departamento de tecnologías de la información a tomar su decisión basándose en los datos disponibles sobre seguridad y no en los reclamos de los vendedores. Éstos afirman ofrecer un entorno seguro cuando en realidad no lo hacen. Recuerde que la certificación CC prueba que una tercera parte imparcial realizó una evaluación.
**********FIN DE NOTA**********

<Cuerpo texto>Como administrador, debería saber y entender que aunque cuente con un sistema operativo con un alto nivel de certificación con respecto a la seguridad, no significa que su implementación esté a ese nivel.
<Nivel 2>Configuración segura de enrutador
<Cuerpo texto>Una de las cosas más importantes que puede hacer para asegurar la red es proteger el enrutador. Por mucho sentido común que tenga, en algunas ocasiones puede verse desbordado por la prisa de tener configurado el enrutador y pasar a la siguiente tarea. Para configurar un enrutador de forma segura, debería hacer lo siguiente:
<Sep-med>* **Cambiar la contraseña predeterminada:** La contraseña del administrador se establece antes de que el enrutador abandone la fábrica. Tiene que asumir que cualquier individuo malintencionado que quiera acceder a su red conoce las contraseñas predeterminadas fijadas por fábrica. Recurra a buenos principios de contraseñas (alfanuméricas, más de ocho caracteres, etc.) y cámbielas por un valor que solo conozcan quienes sea necesario.
* **Configuración avanzada:** Estas opciones variarán dependiendo del fabricante y el tipo de enrutador, pero suelen incluir ajustes para bloquear solicitudes ping o realizar un filtrado MAC, entre otros. Todas estas cuestiones, que se tratan en otros apartados de este libro, es necesario aplicarlas a la configuración del enrutador del mismo modo que las aplica en otro lugar.
* **Mantener el *firmware* actualizado:** Los fabricantes de enrutadores suelen publicar revisiones cuando se descubre algún problema. Es necesario que las aplique en el enrutador para eliminar cualquier incursión de seguridad que pueda existir.
<Cuerpo texto>No olvide que siempre debe guardar una copia de seguridad de la configuración de su enrutador antes de realizar cambios significativos. En concreto, la actualización de *firmware* proporciona una vuelta atrás en caso de que algo vaya mal.
<Nota>**Nota:** Los enrutadores Cisco suelen utilizar uno de estos tipos de contraseñas distintas para sus cuentas: Tipo 7 y MD5 (*Message-Digest Algorithm 5*, Algoritmo de resumen del mensaje 5). Las contraseñas de Tipo 7 usan un cifrado débil y solo se consideran superiores a las de Tipo 0, que son texto sin cifrar. Por este motivo, son muy fáciles de descifrar con *shareware/freeware*, que están disponibles sin problema, y, por lo tanto, debería evitarse. El cifrado de contraseñas MD5 solo utiliza un algoritmo y está configurado en IOS (*Internetwork Operating System*, Sistema operativo de interconexión de redes) usando el comando habilitado secreto.
<Nivel 1>Resumen
<Cuerpo texto>Este capítulo se centra en el control de acceso y la administración de identidad. La diferencia clave entre la autenticación y la identificación es que la primera significa que alguien tiene información precisa, mientras que la segunda implica que dicha información está en posesión del individuo correcto.
La forma de autenticación más básica se conoce como SFA (*Single Factor Authentication*, Autenticación de factor único) porque solo se comprueba un grupo de valores. Para incrementar la seguridad, es necesario pasar a la autenticación de varios factores, que implica la comprobación de dos o más valores.
Este capítulo analiza los distintos tipos de servicio de autenticación, incluyendo RADIUS y las diferentes variaciones de TACACS. Además, se han tratado los protocolos de túnel, las tarjetas inteligentes, así como otros medios de control de acceso.
La línea básica de seguridad proporciona un método estandarizado para evaluar las capacidades de seguridad de productos concretos. Nunca considere que un sistema operativo o una aplicación está seguro hasta que lo compruebe con el estándar EAL, que proporciona siete niveles de certificación. EAL 4 es el nivel recomendado para proporcionar una seguridad razonable para sistemas operativos comerciales.
Las ACL se están implementando en los dispositivos de red y sistemas para habilitar el control de acceso a sistemas y usuarios. Estas permiten ignorar sistemas individuales, usuarios o direcciones IP.
<Nivel 1>Ideas clave para el examen
<Cuerpo texto>A continuación, incluimos las ideas clave que debe recordar para el examen Security+:
<Sep-med>* **Roles de control de acceso:** Los tres roles principales son MAC, DAC y RBAC. MAC (*Mandatory Access Control*, Control de acceso obligatorio) establece métodos de control de acceso rígidos en la organización. DAC (*Discretionary Access Control*, Control de acceso discrecional) permite flexibilidad en el control de acceso. RBAC (*Role-Based Access Control*, Control de acceso basado en roles) se basa en el rol que el individuo o departamento tiene en la organización. En un cuarto tipo de control de acceso, RBAC (*Rule-Based Access Control*, Control de acceso basado en reglas), se utilizan las opciones de las políticas de seguridad establecidas con anterioridad para tomar todas las decisiones.
* **Características de las tecnologías de conectividad disponibles y capacidades de seguridad asociadas a ella:** Acceso remoto, PPP, protocolos de túnel y VPN serán sus herramientas principales. PPTP y L2TP son dos de los protocolos más frecuentes que se utilizan para el tunelado. Aunque IPSec no es un protocolo de túnel, proporciona cifrado para este tipo de protocolos. Se suele utilizar para mejorar la seguridad de túnel.
* **Funcionamiento de ACL:** Las ACL (*Access Control Lists*, Listas de control de acceso) se utilizan para identificar sistemas y especificar qué usuarios, protocolos o servicios se permiten. Los sistemas basados en ACL pueden emplearse para evitar el acceso de usuarios no autorizados a servicios vulnerables.
* **Ventajas de las tecnologías de autenticación disponibles:** Tiene muchas herramientas a su disposición para establecer procesos de autenticación. Algunas empiezan por una contraseña y un ID de usuario. Otras conllevan dispositivos o características físicas de las personas que están solicitando la autenticación.
* **Diferencias y características de las tecnologías disponibles:** Puede segmentar una red y crear redes VLAN para mejorar la seguridad. NAT solo presenta una dirección de Internet al mundo, ocultando los demás elementos de la red. El tunelado le permite realizar conexiones relativamente seguras con otras redes que utilicen Internet.
<Nivel 1>Prueba de evaluación

<Sep-med>1. Se ha comunicado a gran parte del personal de ventas de su cliente que ya no van a informar a la oficina a diario. A partir de ahora, pasarán la mayoría del tiempo en carretera llamando a los clientes. Para ello, se ha facilitado un portátil a cada uno de los miembros del personal de ventas y se les ha pedido que se conecten por las noches a través de una conexión remota. ¿Cuál de los siguientes protocolos se utiliza de forma generalizada como protocolo de transporte para conexiones remotas de Internet?
A. SMTP. **B.** PPP. **C.** PPTP. **D.** L2TP.
2. ¿Qué protocolo es inadecuado para conexiones VPN WAN?
A. PPP. **B.** PPTP. **C.** L2TP. **D.** IPSec.
3. Le han comunicado que pronto se le trasladará a otro lugar. Antes de irse, va a realizar una auditoría en la red y a justificar todo lo que está en uso y por qué. El siguiente administrador utilizará esta documentación para mantener la red en funcionamiento. ¿Cuál de los siguientes no es un protocolo de túnel pero es probable que lo utilicen los protocolos de tunelado por cuestiones de seguridad de red?
A. IPSec. **B.** PPTP. **C.** L2TP. **D.** L2F.
4. Se ha comprobado que el método actual para solicitar el acceso, definido de forma estricta sobre cada objeto, es demasiado voluminoso para el entorno. Desde la administración, se ha tomado la decisión de reducirlo un poco. ¿Qué modelo de acceso permite a los usuarios algo de flexibilidad con el propósito de compartir la información?
A. DAC. **B.** MAC. **C.** RBAC. **D.** MLAC.
5. Un administrador novel recién contratado asumirá su posición de forma temporal mientras usted asiste a un congreso. Está intentando explicarle las bases de seguridad en el menor tiempo posible. ¿Cuál de las siguientes opciones sería más apropiada para describir una ACL?
A. Las ACL proporcionan control de acceso individual a los recursos. **B.** Las ACL no se utilizan en sistemas modernos. **C.** El proceso ACL es dinámico por naturaleza. **D.** Las ACL se utilizan para autenticar a los usuarios.
6. ¿LDAP es un ejemplo de cuál de las siguientes opciones?
A. Protocolo de acceso a directorio. **B.** IDS. **C.** Entorno de desarrollo de aplicaciones modelo con fases. **D.** Servidor de archivo.
7. De repente, la administración se preocupa por la seguridad. Como administrador de red experto, le han pedido que sugiera qué cambios se deberían implementar. ¿Cuál de los siguientes métodos de acceso recomendaría si el método va a ser uno que se fundamenta, básicamente, en el acceso preestablecido y no puede modificarse por los usuarios?
A. MAC. **B.** DAC. **C.** RBAC. **D.** Kerberos.
8. El administrador de su oficina se está preparando para realizar copias de seguridad del servidor. ¿Qué método de autenticación sería ideal para esta situación?
A. MAC. **B.** DAC. **C.** RBAC. **D.** *Tokens* de seguridad.
9. Se le ha asignado como tutor de un administrador novel y quieren que aprenda rápido. Imagine que le está explicando el tema de la autenticación. ¿Qué método utiliza un KDC para la autenticación de los usuarios, programas o sistemas?
A. CHAP. **B.** Kerberos. **C.** Biometría. **D.** Tarjetas inteligentes.
10. Tras un análisis de riesgos exhaustivo, se ha incrementado el valor de los datos de su empresa. De acuerdo con ello, se espera que implementen soluciones de autenticación que lo reflejen. ¿Cuál de los siguientes métodos de autenticación utiliza más de un proceso para iniciar sesión?
A. Varios factores. **B.** Biometría. **C.** Tarjetas inteligentes. **D.** Kerberos.
11. Es el administrador de una conocida empresa. Debido a las numerosas expansiones, el tamaño de la red ha crecido exponencialmente en los últimos dos años. ¿Cuál de los siguientes es un conocido método para descomponer redes en redes privadas más pequeñas que pueden coexistir en el mismo cableado y aun así ser ajenas la una a la otra.
A. VLAN. **B.** NAT. **C.** MAC. **D.** Zona de seguridad.
12. ¿Qué tecnología permite que se realice una conexión entre dos redes utilizando un protocolo seguro?
A. Túnel. **B.** VLAN. **C.** Internet. **D.** Extranet.
13. Su empresa proporciona datos médicos a una base de datos de doctores de todo el mundo. Debido a su naturaleza confidencial, es imprescindible establecer una autenticación para cada sesión que solo sea válida para esta. ¿Cuál de los siguientes métodos de autenticación proporciona credenciales que solo son válidas durante una sesión?
A. *Tokens*. **B.** Certificado. **C.** Tarjeta inteligente. **D.** Kerberos.
14. ¿Cuál de los siguientes es el término que se utiliza siempre que dos o más partes se autentican entre sí?
A. SSO. **B.** Autenticación de varios factores. **C.** Autenticación mutua. **D.** Túnel.
15. ¿Cuál de las siguientes áreas de seguridad engloba NAC (*Network Access Control*, Control de acceso de red)?
A. Seguridad física. **B.** Seguridad operativa. **C.** Seguridad de administración. **D.** Seguridad de la tríada.
16. Ha añadido un nuevo dominio subordinado a su red. Como resultado, este ha adoptado las relaciones de confianza con los otros dominios existentes en el dominio principal. ¿Qué es responsable de esto?
A. Acceso LDAP. **B.** Acceso XML. **C.** Acceso cruzado. **D.** Acceso transitivo.
17. ¿A qué se recurre cuando una persona reclama que es usuario pero que no puede autenticarse, por ejemplo, porque ha perdido la contraseña?
A. Prueba de identidad. **B.** Ingeniería social. **C.** Transversal de directorio. **D.** Solicitud de varios sitios.
18. ¿Cuál de los siguientes es un entorno orientado a cliente y servidor que funciona de forma similar a RADIUS?
A. HSM. **B.** TACACS. **C.** TPM. **D.** ACK.
19. ¿Qué está implícito en el extremo de cada lista de control?

A. Privilegio mínimo. **B.** Separación de tareas. **C.** Denegación implícita. **D.** Permiso explícito.

20. ¿Cuál de los siguientes es un tipo de tarjeta inteligente expedida por el Departamento de Defensa estadounidense como tarjeta general de identificación/autenticación destinada a personal militar, contratistas y empleados que no pertenecen a este departamento?

A. PIV. **B.** POV. **C.** DLP. **D.** CAC.

<Nivel 1>Respuestas de la prueba de evaluación

1. B. PPP puede pasar numerosos protocolos y hoy en día se utiliza de forma generalizada como protocolo de transporte para conexiones remotas.
2. A. PPP no proporciona seguridad y todas las actividades son inseguras. PPP está destinado principalmente a conexiones remotas y nunca debería utilizarse con conexiones VPN.
3. A. IPSec proporciona seguridad de red para los protocolos de túnel. Puede emplearse con muchos protocolos además de TCP/IP y tiene dos modos de seguridad.
4. A. DAC permite alguna flexibilidad en las capacidades para compartir información en la red.
5. A. Las listas de control de acceso permiten una entrada muy controlada e individualizada a los recursos de una red. Una ACL también puede emplearse para excluir un sistema, una dirección IP o a un usuario en particular.
6. A. LDAP es un protocolo de acceso a directorio que se utiliza para publicar información sobre los usuarios. Es el equivalente informático a un listín telefónico.
7. A. MAC está orientado hacia un acceso establecido con anterioridad. Suelen establecerlo los administradores de red y los usuarios no pueden modificarlo.
8. C. RBAC permite que personas específicas se asignen a roles determinados con privilegios concretos. Un operador de copias de seguridad necesitaría privilegios administrativos para realizar una copia de seguridad del servidor. Este privilegio estaría limitado a este rol y no estaría presente durante las funciones cotidianas del empleado.
9. B. Kerberos utiliza un KDC para autenticar a un principal. El KDC proporciona una credencial que pueden utilizar todos los servidores y aplicaciones que tengan habilitado Kerberos.
10. A. Un método de autenticación de varios factores emplea dos o más procesos para iniciar sesión. Un método de dos factores podría utilizar tarjetas inteligentes y biometría.
11. A. Una red VLAN descompone redes complejas en redes más pequeñas. Estas pueden coexistir en el mismo cableado y estar ajenas la una a la otra. Necesitaría un enrutador u otro tipo de dispositivo de enrutamiento para conectar las VLAN.
12. A. El túnel permite a una red realizar una conexión segura con otra red a través de Internet u otra red. Los túneles suelen ser seguros y se presentan como extensiones de las dos redes.
13. A. Los *tokens* se crean cuando un usuario o sistema se autentica con éxito. Cuando la sesión termina, este se destruye.
14. C. Siempre que dos o más partes se autentican entre sí se conoce como autenticación mutua.
15. B. Las cuestiones de seguridad operativa incluyen NAC, autenticación y topologías de seguridad una vez que se ha completado la instalación de red.
16. D. Existe el acceso transitivo entre los dominios y crea esta relación.
17. A. Se recurre a la prueba de identidad cuando una persona reclama que es usuario pero que no puede autenticarse, por ejemplo, porque ha perdido la contraseña.
18. B TACACS es un entorno orientado a cliente y servidor que funciona de forma similar a RADIUS.
19. C. Una denegación implícita está implícita en el extremo de cada lista de control.
20. D. Un tipo de tarjeta inteligente es CAC. Estas tarjetas las expide el Departamento de Defensa estadounidense como tarjeta general de identificación/autenticación destinada a personal militar, contratistas y empleados que no pertenecen a este departamento

Capítulo 10. Seguridad física y basada en hardware

<Cuerpo texto>En este capítulo se tratan los siguientes objetivos del examen CompTIA Security+:
<Sep-med>2.6 Explicar el impacto y el uso correcto de controles medioambientales.
3.6 Analizar y diferenciar las distintas técnicas de mitigación y disuasión.
4.2 Llevar a cabo los procedimientos adecuados para establecer la seguridad host.
5.2 Explicar los conceptos fundamentales y las prácticas más adecuadas en relación con la autentificación, la autorización y el control de acceso.
<Cuerpo texto>Este capítulo le ayudará a entender la importancia tanto de las medidas de seguridad física como de los controles de acceso, barreras físicas y sistemas biométricos. También describe el entorno que necesitan sus sistemas para que sean seguros y funcionales. Además, trata la seguridad de red y se centra en las zonas de seguridad y particiones.
Las medidas de seguridad física evitan los accesos no autorizados a sus sistemas. De este modo, impide que un usuario llegue físicamente a un sistema o dispositivo sin su consentimiento. La mayoría de los sistemas de red han desarrollado altos niveles de sofisticación y seguridad frente a intrusos. No obstante, estos sistemas suelen ser vulnerables a ataques internos, sabotajes y malos usos. Si un impostor tiene acceso físico a sus sistemas, nunca estarán seguros.
<Nivel 1>Implementar el control de acceso
<Cuerpo texto>El control de acceso es una parte de la seguridad física. Los sistemas deben funcionar en entornos controlados para que sean seguros. Éstos deben estar protegidos del acceso de intrusos tanto como sea posible. Las consolas de los sistemas informáticos pueden ser un punto vital de vulnerabilidad ya que pueden llevarse a cabo funciones administrativas desde ellas. Estas y los propios sistemas deben estar preservados contra la entrada física. Hay dos áreas que le ayudan a incrementar el control de acceso y hacer que el sistema sea seguro. Se trata de las barreras físicas y la biometría. Ambas se explican en las siguientes secciones.
<Nivel 2>Barreras físicas
<Cuerpo texto>Un aspecto clave del control de acceso está relacionado con las barreras físicas. El objetivo de estas es evitar la entrada a los ordenadores y a los sistemas de red. Las implementaciones de barreras físicas más efectivas requieren que se supere más de una de esta para obtener el acceso. Este tipo de enfoque se conoce como sistema de barrera múltiple.
Lo ideal es que sus sistemas cuenten con un mínimo de tres barreras físicas:
<Sep-med>* **Perímetro:** Se refiere a la entrada externa al edificio que está protegida por alarmas antirrobo, muros externos, vallas y vigilancia, entre otros. Debería combinarse con el uso de una lista de acceso que identifique físicamente quién puede entrar a una instalación y que un guardia o alguien que esté al mando pueda verificarlo.
* **Candados:** Una puerta con candado para proteger el centro informático. También tendría que emplear dispositivos como tarjetas de identificación, llaveros con pantallas LCD (*Liquid Crystal Display*, Pantalla de cristal líquido) o claves para obtener acceso.
* **Entrada:** Se refiere al acceso a la habitación en la que están los ordenadores. Debería tener otra puerta con candado cuidadosamente monitorizada. Aunque intente mantener a los intrusos fuera de las otras dos barreras, muchas de las personas que entren al edificio podrían hacerse pasar por quien no son: técnicos de calefacción o representantes de los propietarios, entre otros. Pese a que éstos puedan pasar las dos primeras barreras, deberían detenerse ante la puerta con candado de la sala informática.
<Cuerpo texto>Cada una de estas entradas puede asegurarse, monitorizarse y protegerse de forma individual con sistemas de alarma. La figura 10.1 ilustra este concepto.
**********10_001.tif**********
<Pie figura>**Figura 10.1.** El modelo de seguridad de tres capas.
<Nota>**Nota:** El lector de proximidad es un término comodín para cualquier ID o lector de tarjetas capaz de leer las tarjetas de proximidad. Estas llevan distintos títulos pero en realidad solo son tarjetas RFID (*Radio Frequency Identification*, Identificación por radiofrecuencia) que pueden leer cuando están cerca de un lector y no tienen por qué estar en contacto con nada. Los lectores funcionan con tarjetas inteligentes de 13.56 MHz y tarjetas de proximidad de 125 kHz, y puede abrir controles, puertas y otras medidas de seguridad físicas, una vez que se lee la señal.
<Cuerpo texto>Aunque estas barreras no siempre detendrán a los intrusos, pueden reducir su velocidad lo suficiente como para que las fuerzas del orden puedan responder antes de que una entrada ilegal se complete. Una vez dentro, un sitio realmente asegurado debería depender de un *token* físico o de la biometría para acceder a los recursos de red.
**********INICIO DE NOTA**********
<Nivel 3>Token físicos
<Nota>**Nota:** Los *token* físicos son todo aquello que un usuario debe tener para acceder a los recursos de red y suelen estar asociados con dispositivos que habilitan a las personas autorizadas para generar una contraseña de un solo uso que autentique su identidad. SecurID, de RSA, es uno de los ejemplos más conocidos de *token* físico y puede encontrar información sobre él en http://www.rsa.com/node.aspx?id=1156.
No importa lo seguro que piense que es su sistema, nunca podrá detener a todo el mundo. No obstante, su objetivo es detener el mayor número posible de intentos y, como mínimo, reducir la velocidad de los más sofisticados. Por ejemplo, la puerta frontal de su casa puede tener un candado y un cerrojo. Esta seguridad mínima es suficiente para convencer a la mayoría de ladrones de que vayan a otro sitio menos seguro. Un profesional que está empeñado en entrar en su casa, siempre podría llevar una sierra mecánica o una herramienta similar para abrir la puerta.
**********FIN DE NOTA**********
<Nivel 3>Mantrap

<Cuerpo texto>Las instalaciones de alta seguridad emplean un tipo de mecanismo de control de acceso intermedio conocido como *mantrap* (cepo), también se suele escribir *man-trap*. Este requiere identificación visual y autenticación para obtener el acceso, y hace que sea más difícil que varias personas accedan a la instalación porque solo permite que entren uno o dos individuos al mismo tiempo. Se suele diseñar para contener físicamente a una persona no autorizada, posiblemente hostil. La figura 10.2 es un ejemplo de ello. Observe que en este caso la verificación visual se consigue empleando un guarda de seguridad. Un *mantrap* desarrollado correctamente incluye un cristal blindado, puertas de alta resistencia y candados. En entornos de alta seguridad y militares, se colocaría, además, un guarda armado y cámaras de vigilancia. Cuando una persona entre en las instalaciones, pueden requerirse medidas adicionales en más accesos.
**********10_002.tif**********
<Pie figura>**Figura 10.2.** Un mantrap en funcionamiento.
<Nota>**Nota:** Algunos *mantrap* incluyen incluso balanzas para pesar a la personas. Aunque esto puede ayudar a identificar a un individuo, estas suelen emplearse para comprobar que no hay nada sospechoso. Si el peso parece demasiado alto, un oficial se asegurará de que no se trata de dos personas que quieren sortear rápidamente la seguridad.
<Nivel 3>Seguridad del perímetro
<Cuerpo texto>La seguridad del perímetro, con independencia de que sea física o tecnológica, es la primera línea de defensa de su modelo de seguridad. En el caso de que sea un elemento de seguridad física, se pretende evitar el acceso no autorizado a los recursos del edificio o la instalación.
El equivalente de red de la seguridad del perímetro físico tiene como objetivo conseguir en una red lo mismo que se consigue en un edificio. ¿Cómo evita que los intrusos accedan a los sistemas y la información de la red?
En el entorno físico, la seguridad del perímetro se consigue empleando candados, puertas, sistemas de vigilancia y alarmas. Desde el punto de vista funcional, no hay ninguna diferencia con una red que utiliza enrutadores fronterizos, sistemas de detección de intrusos y cortafuegos para evitar el acceso no autorizado. La figura 10.3 ilustra los sistemas autorizados para evitar la intrusión de red.
**********10_003.tif**********
<Pie figura>**Figura 10.3.** Defensa del perímetro de red.
<Cuerpo texto>Pocos serán los sistemas de seguridad que se pongan en funcionamiento y no presenten ninguna debilidad o vulnerabilidad. Con paciencia, un determinado intruso puede desbaratar la mayoría de estos sistemas. Es posible que no se trate de una tarea fácil y que requiera un cuidadoso plan y estudio. Sin embargo, un enemigo puede encontrar la manera. Por esta razón, los factores disuasivos son tan importantes.
Si quiere desalentar a los intrusos para que no irrumpan en su sistema, puede instalar candados reforzados en las puertas, sistemas de alarmas con código y contactos magnéticos en puertas y ventanas. Recuerde que no siempre podrá evitar que una persona ajena entre en el edificio. Sin embargo, puede hacer que la intromisión sea más arriesgada y más fácil de descubrir si se produce.
<Nota>**Truco:** No pase por alto lo obvio. Añadiendo un guardia de seguridad en la puerta frontal, tendrá gran parte del camino recorrido para mantener a un intruso fuera.
**********INICIO DE NOTA**********
<Nivel 3>Sortear la seguridad
<Nota>Recientemente, una pequeña empresa observó que el nivel del tráfico de red era muy alto a última hora de la tarde y a primera hora de la mañana. No podían encontrar una razón relacionada con la red para averiguar lo que estaba ocurriendo. Tras realizar una investigación, el asesor de red descubrió que un empleado a tiempo parcial había establecido el servidor de un juego de varios usuarios en su oficina. Este se encendía después de las diez de la noche y se desactivaba a las cinco y media de la madrugada. El servidor estaba escondido debajo de un escritorio y prestaba soporte a unos treinta jugadores locales. El trabajador no tenía clave para el edificio, por lo tanto, se realizó otra investigación para descubrir cómo accedía al edificio durante esas horas. Había candados electrónicos en las entradas externas y era necesario pasar una tarjeta para abrir las puertas. No obstante, los candados estaban diseñados para desbloquearse cuando alguien salía del edificio.
La investigación concluyó que el empleado y un amigo habían diseñado cómo deslizar una pieza de cartulina bajo una de las puertas externas. Esto activaba sus mecanismos y la desbloqueaba. Los intrusos se aprovechaban de esta debilidad en las puertas para acceder durante horas sin utilizar una tarjeta y, a continuación, empleaban el servidor para ejecutar juegos en su oficina.
**********FIN DE NOTA**********
<Nivel 3>Seguridad de hardware
<Cuerpo texto>La seguridad de hardware implica aplicar modificaciones de seguridad físicas para asegurar los sistemas y evitar que se pierdan. No pase el tiempo preocupándose por los intrusos procedentes de la red y no olvide la obvia necesidad de la seguridad física.
Añadir un candado entre un portátil y un escritorio impide que alguien se lo lleve y, con ello, una copia de la base de datos de clientes. Por ejemplo, es aconsejable incluir una ranura en los portátiles en la que se puede añadir un candado para evitar que los quiten del lugar en el que están, como los que aparecen en la figura 10.4.
**********10_004.tif**********
<Pie figura>**Figura 10.4.** Un cable en la ranura de seguridad evita que el portátil se quite con facilidad.
<Cuerpo texto>Cuando se trata de modelos de escritorio, añadir un candado en la carcasa trasera puede evitar que un intruso con acceso físico se haga con el disco duro o dañe los componentes internos. El candado que se conecta a través de la ranura también puede derivar en un calve conectado a un escritorio o a otra superficie sólida para impedir que se robe el PC completo. En la figura 10.5, puede observar un ejemplo de este tipo de configuración.
**********10_005.tif**********

<Pie figura>**Figura 10.5.** Puede emplear un cable para evitar que un ordenador de escritorio se robe fácilmente.
<Cuerpo texto>Además de colocar un cable en el escritorio, también puede poner un extremo de este en el monitor si existe riesgo de robo de periféricos. En la figura 10.6, aparece un ejemplo de ello.
**********10_006.tif**********
<Pie figura>**Figura 10.6.** Si hay riesgo de robo, coloque un extremo del cable en el monitor y el otro en la máquina de escritorio haciendo un agujero en la mesa de trabajo.
<Cuerpo texto>También debería considerar el uso de armarios con candados para proteger las copias de seguridad, la documentación y otros artefactos que pudieran perjudicarle si cayeran en otras manos. Los *rack* bloquean los servidores que se instalan en estos armarios con el fin de evitar que alguien lo coja y se lo lleve.
<Nota>**Nota:** Aunque esta explicación se centra en la seguridad física, no pase por alto el cifrado como medio para incrementar la seguridad de los datos en caso de que roben un sistema de escritorio o un portátil. También debe barajar la posibilidad de alejar los discos duros de áreas que sean difíciles de monitorizar y hacer que todos los datos se almacenen en la red.
<Nivel 2>Zonas de seguridad
<Cuerpo texto>Una zona de seguridad es un área de un edificio en la que el acceso se monitoriza y se controla de forma individual. Una gran red, como una gran planta física, puede contar con muchas zonas que requieran acceso restringido. En un edificio, las plantas, las secciones de las plantas e incluso las oficinas pueden descomponerse en áreas más pequeñas. Estas se conocen como zonas de seguridad. En el entorno físico, cada planta se descompone en zonas independientes. Un sistema de alarma que identifica una zona de intrusión puede informar al personal de seguridad de la localización de un agresor en el edificio. La notificación de zona comunica la seguridad por dónde empezar a buscar cuando alguien entre.
El concepto de zonas de seguridad es tan antiguo como el de seguridad. La mayoría de alarmas antirrobo permiten la creación de zonas individuales dentro de un edificio o residencia y el personal de seguridad las trata de forma independiente. En una residencia, sería normal establecer el dormitorio como una zona independiente para detectar el movimiento que se produzca allí, mientras que otras partes de la casa pueden contar con un sensor de movimiento. En el ejercicio 10.1 aprenderá cómo evaluar su entorno.
**********Inicio ejercicio**********
<Nivel 4>Ejercicio 10.1. Zonas de seguridad en el entorno físico
<Cuerpo texto>Como administrador de seguridad, tendrá que evaluar su lugar de trabajo y pensar las zonas físicas que deberían existir según los tipos de individuos que puedan estar presentes. Si su lugar de trabajo ya está dividido en zonas, olvide lo que hay ya hecho y empiece de cero. Responda a las siguientes preguntas:
<Sep-med>1. ¿Qué áreas representan la dimensión física de su lugar de trabajo (edificios, plantas u oficinas, entre otros)?
2. ¿Qué áreas son accesibles a todo el mundo, desde los administradores hasta los usuarios? ¿Pueden los visitantes dejar el área de recepción sin escolta y, si lo hacen, a dónde se dirigen (a los servicios, a la sala de personal, etc.)?
3. ¿En qué áreas se permite a los usuarios moverse libremente? ¿Está seguro de que ningún visitante o invitado podría entrar a otra áreas?
4. ¿A qué zonas se les permite entrar a los administradores y a cuáles no? ¿A la habitación del servidor? ¿A los armarios de cableado? ¿Cómo mantiene fuera a los usuarios y verifica que solo entran los administradores?
5. ¿Hay conexiones de pared, accesos de red o las redes Wi-Fi disponibles en los lugares a los que acceden los visitantes?
6. ¿Hay otras áreas que necesiten asegurarse para entidades más allá de la distinción usuario/administrador (como grupos)?
<Cuerpo texto>Cuando tenga esta información, debería buscar formas de abordar las debilidades que haya encontrado. Evalúe su entorno de forma rutinaria para comprobar que las zonas que ha establecido en su plan de seguridad siguen siendo relevantes. Siempre debe empezar desde cero y simular que no hay áreas. A continuación, verifique que las que existen son las mismas que ha creado a partir de este ejercicio.
**********Fin ejercicio**********
<Cuerpo texto>El equivalente de red de una zona de seguridad es una zona de seguridad de red. Ambas realizan la misma función. Si divide una red en secciones más pequeñas, cada zona tendrá sus propias consideraciones y medidas de seguridad, al igual que un área de seguridad física. La figura 10.7 ilustra una red grande divida en tres zonas más pequeñas. Observe que la primera también contiene un área más pequeña en la que se almacena la información de alta seguridad. Esta organización permite que las capas de seguridad se construyan alrededor de información confidencial. La división de la red se consigue implementando redes LAN virtuales (VLAN) y estableciendo DMZ (*Demilitarized Zones*, Zona desmilitarizada).
**********10_007.tif**********
<Pie figura>**Figura 10.7.** Zonas de seguridad de red.
<Nivel 2>Particiones
<Cuerpo texto>El proceso para dividir una red es el mismo que en un edificio. En este, existen los tabiques para dirigir el tránsito de visitantes, proporcionar control de acceso y separar áreas funcionales. Este proceso permite que la información y la propiedad estén bajo candado y llave físicos.
A través de las particiones, puede aislar una entidad de otra. Esta puede ser física (una habitación puede separarse de otra en un edificio) o lógica (los que pueden acceder a un conjunto de datos no pueden acceder a otro). Esta explicación se elabora a partir de las posibilidades que ofrecen las particiones.
<Nota>**Truco:** Las particiones pueden ser estructuras temporales o permanentes.

<Cuerpo texto>Los recibidores de un edificio de oficinas suelen construirse de forma distinta al espacio interno. Acostumbran a ser más resistentes al fuego y se conocen como corredores. Éstos permiten que las personas que están en el edificio escapen en caso de incendio. Las paredes del corredor van desde el suelo hasta el techo, mientras que los tabiques internos pueden acabar antes de este (la mayoría de los edificios de oficinas tienen un falso techo para almacenar la iluminación, el cableado y las tuberías).
Las particiones de red realizan la misma función para una red que las particiones físicas de un edificio. Los edificios tienen tabiques físicos y la partición de red conlleva la creación de redes privadas dentro de redes más grandes. Estas divisiones pueden aislarse entre sí utilizando enrutadores y cortafuegos.
Por lo tanto, aunque los sistemas de red estén todos conectados a través del cableado, la vista funcional es la de muchas redes más pequeñas. La figura 10.8 muestra una red fragmentada. Es importante entender que, a menos que un dispositivo físico (por ejemplo, un enrutador) separe estas particiones de red, todas las señales se compartirán a través del cableado.
Este dispositivo realiza la misma función que un recibidor o una puerta con candado, desde una perspectiva puramente física.
**********10_008.tif**********
<Pie figura>**Figura 10.8.** Particiones que separan las redes entre sí en una red más grande.
<Nota>**Nota:** Las particiones y las zonas de seguridad son básicamente intercambiables. En general, las primeras son más específicas que las segundas, pero no siempre es así. En una instalación típica, una zona engloba una planta, mientras que una partición podría incluir una habitación.
**********INICIO DE NOTA**********
<Nivel 3>Instalar dispositivos biométricos
<Nota>Le pedido que solucione el problema de los usuarios que olvidan las tarjetas inteligentes que les dan acceso al centro informático. Casi todos los días le ocurre a alguien. Esto puede provocar un alto grado de trastorno en el lugar de trabajo porque otra persona tiene que volver a expedir constantemente las tarjetas inteligentes. La empresa ha intentado todo. Incluso está pensando en despedir al personal que olvide sus tarjetas. ¿Qué recomendaría a la compañía?
Investigue si hay dispositivos biométricos (como escáneres de huella) o candados de acceso que puedan usarse en lugar de las tarjetas inteligentes para el acceso. Estos dispositivos permitirán a los empleados que olviden sus tarjetas entrar a zonas a las que están autorizados.
**********FIN DE NOTA**********
<Nivel 2>Biometría
<Cuerpo texto>Los sistemas biométricos utilizan un tipo de característica biológica única para identificar a una persona, por ejemplo huellas dactilares, patrones de retina y huellas de manos. Algunos de los dispositivos que se utilizan son los escáneres de manos, de retina, aplicaciones de reconocimiento facial y programas de reconocimiento de pulsaciones, que pueden emplearse como parte de los mecanismos de control de acceso. Éstos deberían combinarse con sistemas informáticos con seguridad habilitada que registren todos los intentos de acceso. También tendría que estar bajo vigilancia con el fin de evitar que los individuos los esquiven.
Estas tecnologías cada vez son más fiables y se implementarán de forma generalizada en los próximos años. En la actualidad, muchos de los portátiles que se venden incorporan un lector de huella. Los costes asociados a estas tecnologías han descendido considerablemente en estos últimos años. Una de las mejores fuentes de información independiente sobre el desarrollo en este campo es http://www.biometricnews.net. En esta página Web encontrará enlaces a las publicaciones y a sus blogs.
**********INICIO DE NOTA**********
<Nivel 3>Evaluar su sistema de seguridad
<Cuerpo texto>Le han pedido que evalúe el sistema de seguridad de su edificio. El presidente le ha elegido a usted porque sabe de ordenadores y, al fin y al cabo, estas nuevas alarmas están informatizadas.
Analizando el entorno, observa que hay un único panel de control para todo el edificio. En el recibidor principal encuentra algunos detectores de movimiento. Aparte de eso, no se han instalado más componentes adicionales de seguridad.
Esta situación es bastante normal en una pequeña empresa. Sin embargo, podría recomendar mejorar el sistema añadiendo detectores de movimiento en cada recibidor principal, instalar cámaras de monitorización de vídeo (también conocidos como vigilancia) y CCTV (*Closed-Circuit Television*, Circuito cerrado de televisión) en todas las entradas. La mayoría de las cámaras CCTV de seguridad/vigilancia tienen capacidades PTZ (*Pan, Tilt, and Zoom*, Panorámica, ángulo y zoom) y, en ocasiones, se basan en el sonido o el movimiento. También debería recomendar que se actualice la seguridad del perímetro añadiendo sensores de contacto en todas las puertas y ventanas de la planta baja.
Siempre debe analizar el edificio desde un enfoque que contemple diversos puntos de vista. Incorpore tantos elementos como sean necesarios: seguridad de perímetro, zonas de seguridad y vigilancia.
**********FIN DE NOTA**********
<Nivel 1>Mantenimiento del entorno y de los controles de energía
<Cuerpo texto>La localización de la instalación informática es crítica para su seguridad. Esta tiene que colocarse en una ubicación que se pueda proteger físicamente. Además, debería tener capacidades propias para gestionar la temperatura, la humedad y otros factores del entorno necesarios para la salud de sus sistemas informáticos. Las siguientes secciones analizan el entorno y los sistemas de energía.
<Nivel 2>Monitorización del entorno
<Cuerpo texto>Muchos sistemas informáticos requieren controles de temperatura y humedad para una mayor fiabilidad del servicio. Los servidores más grandes, el equipo de comunicaciones y los conjuntos de discos generan

cantidades de calor considerables. Esto ocurre sobre en grandes sistemas y miniordenadores más antiguos. Un sistema ambiental para este tipo de equipo es un gasto significativo que va más allá de los costes del sistema informático. Afortunadamente, los equipos más recientes operan en un rango más amplio de temperaturas y, la mayoría están diseñados para funcionar en un entorno de oficina.
Si los sistemas informáticos que están bajo su responsabilidad requieren consideraciones ambientales especiales, tendrá que establecer controles de refrigeración y humedad. Lo ideal es que los sistemas se encuentren en el centro del edificio y los conductos estén separados del resto del sistema HVAC (*Heating, Ventilation, and Air Conditioning*, Calefacción, ventilación y aire acondicionado). En los edificios modernos, es una práctica común utilizar un entorno de aire acondicionado basado en zonas, que permite que se desactive una planta cuando el edificio no está siendo ocupado. En general, una sala informática requerirá un control ambiental a tiempo completo.
<Nota>**Nota:** Los sistemas ambientales deberían estar monitorizados para evitar que el nivel de humedad del centro informático descienda por debajo del cincuenta por ciento. Es probable que se produzcan daños electroestáticos cuando los niveles de humedad sean demasiado bajos.
<Cuerpo texto>Los controles de humedad evitan la acumulación de electricidad estática en el entorno. Si la humedad desciende por debajo del cincuenta por ciento, los componentes electrónicos pueden sufrir daños electroestáticos. La mayoría de los sistemas ambientales también regulan la humedad. Sin embargo, un sistema que funcione mal puede provocar que la humedad se extraiga casi por completo de la habitación. Compruebe que todos los sistemas ambientales se supervisan de forma regular.
Las preocupaciones en cuanto al entorno también incluyen consideraciones sobre los daños del agua y las inundaciones, así como la prevención de incendios. Las salas informáticas tienen detectores de incendios y humedad. La mayoría de los edificios de oficinas poseen tubos para el agua y otros sistemas para transportar humedad en el techo. Si estos tubos se rompen (lo que es frecuente en terremotos pequeños), la sala de informática se inundará. Tenga en cuenta que el agua y la electricidad no hacen buenas migas, por lo que los monitores de humedad acabarían automáticamente con la energía de una sala informática si se detectara la humedad. El profesional de la seguridad debería conocer dónde están las llaves de paso para cortar el agua.
El fuego, independientemente de su magnitud, puede dañar los sistemas informáticos. Aparte de los incendios, que pueden fundir plástico y metal, el humo puede impregnar los ordenadores. Las partículas de humo son lo bastante grandes como para cubrir la cabeza de lectura/escritura de un disco duro y provocar la pérdida de datos. Además, los sistemas antiincendios de la mayoría de edificios son agua a presión y esta podría acabar con todo un centro de datos aunque se tratara de un pequeño incendio.
<Nota>**Nota:** Las medidas antiincendios se tratan más adelante.
<Nota>**Truco:** Los tres componentes críticos de un incendio son el calor, el combustible y el oxígeno. Si se elimina algún elemento de esta trilogía, el incendio no es posible. La mayoría de las medidas antiincendios funcionan de acuerdo con este concepto.
<Nivel 2>Sistemas de energía
<Cuerpo texto>Los sistemas informáticos pueden presentar problemas de energía e interferencias. Un ordenador requiere una entrada estable de corriente alterna para producir voltaje de corriente continua que suministre a los sistemas electrónicos. Los sistemas de energía están diseñados para funcionar en un amplio rango de características, ayudar a que el servicio eléctrico sea constante y asegurar que las operaciones sean fluidas.
**********INICIO DE NOTA**********
<Nivel 3>Las pequeñas cosas pueden tener enormes consecuencias
<Nota>El agua puede venir de cualquier parte y necesita estar preparado cuando se produzca alguna fuga. Hace algunos años, una empresa tenía una habitación con un servidor de última generación en la planta alta de su edificio. La temperatura estaba controlada. Justo encima de la habitación del servidor estaba el tejado y, en este, el banco de los aires acondicionados de las seis plantas del edificio. En el transcurso de un fin de semana muy caluroso, las tuberías de desagüe de la condensación de los aires acondicionados se atascaron, se llenaron de agua y se rompieron. El agua pasó por el tejado y entró en la parte alta. Una vez allí, el agua siguió su camino hasta el punto más bajo haciendo un agujero en el techo, justo encima de los servidores. Todo quedó inservible en un breve período de tiempo.
Por muy improbable que parezca, esto sucede más a menudo de lo que pensamos. Cuando ocurra, tendrá que estar preparado y contar con copias de seguridad, cintas, servidores y monitores, entre otros.
**********FIN DE NOTA**********
<Nota>**Nota:** Fluctuaciones importantes en la corriente alterna pueden contribuir a la aparición de una situación conocida como arrastramiento de chips. Éstos se van arrastrando lentamente porque están sin soldar y acaban saliendo de la toma de corriente con el paso del tiempo.
<Cuerpo texto>Los siguientes productos resuelven la mayoría de los problemas que presenta el cableado eléctrico:
<Sep-med>* **Protector de sobretensión o supresor de tensión:** Protege los componentes eléctricos de incrementos momentáneos o instantáneos (llamados picos) en la corriente. La mayoría de supresores de tensión regulan los picos de voltaje enviando a la tierra voltajes superiores a un umbral seguro mediante pequeños dispositivos llamados MOV (*Metal Oxide Varistors*, Varistor metálico). Los supresores de tensión a gran escala suelen encontrarse en los suministros de energía de los edificios o en los puntos de alimentación eléctrica del inmueble. Puede comprar supresores de tensión portátiles como parte de un alargador de cable o un ladrón pero solo suelen ser buenos para un pico. Si se producen oleadas posteriores, puede que el protector no evite que pasen a través de la línea hasta el sistema informático. Se trata de dispositivos pasivos y no tienen ninguna funcionalidad hasta que se producen los picos.
* **Regulador de corriente:** Este es un dispositivo activo que aísla y regula, de forma efectiva,el voltaje de un edificio; controla la energía y la limpia. Los reguladores de corriente suelen incluir filtros, supresores de tensión y

reguladores de voltaje temporales, y pueden activar las reservas de los suministros de energía. Asimismo, pueden formar parte del esquema de energía del edificio en su conjunto. Es frecuente encontrarlos en salas informáticas con un uso exclusivo.

* **Reservas de energía:** Se suelen utilizar en situaciones en las que se necesita una energía continuada y se produce una pérdida de corriente. Estos tipos de sistema se suelen diseñar para breves intervalos de tiempo, por ejemplo, un sistema de reserva de batería, o para más largo plazo, empleado en un UPS (*Uninterruptible Power Supply*, Sistema de alimentación ininterrumpida). Estos sistemas suelen utilizar baterías para proporcionar energía a corto plazo. Las reservas de energía a más largo plazo proceden de generadores que tienen sus propios circuitos para detectar la pérdida de energía. Éstos se activan si se detecta la carencia de corriente y proporcionan energía hasta que se deshabiliten. Los generadores requieren de un breve período de tiempo para empezar a proporcionar corriente y los sistemas de baterías de reserva le ofrecen ese margen para que inicien su funcionamiento. La mayoría de ellos no se desactivan de forma automática cuando se restablece la energía en un edificio. Hay que desactivarlos manualmente. Se trata de algo necesario porque es habitual que se produzcan algunos inicios falsos antes de que se restablezca la corriente.

Gran parte de los generadores de energía funcionan con diésel o gasolina, y requieren un mantenimiento preventivo regular. Estos sistemas no resultan de gran utilidad si no se inician cuando es necesario o si fallan porque no tienen combustible en el motor. Los más modernos se basan en la tecnología de pila de combustible y es probable que resulten mucho más fiables y requieran menos mantenimiento.

<Nivel 2>Protección EMI

<Cuerpo texto>La protección se refiere al proceso para evitar que las emisiones electrónicas de sus sistemas informáticos se empleen para recabar información e impedir que emisiones externas interrumpan las habilidades de procesamiento de sus datos. En una instalación fija, como un centro informático, rodear la sala de informática con una jaula de Faraday puede proporcionar protección electrónica. Esta suele consistir en un campo electromagnético que rodea una habitación y con el cual el conductor se polariza. Debido a esta jaula, pocas señales electromagnéticas pueden entrar o salir de la habitación, y se reduce la posibilidad de que se escuche a hurtadillas una conversación informática. Para verificar la funcionalidad de la jaula, debe comprobar las emisiones RF (*Radio Frequency*, Frecuencia de radio) con dispositivos de medida especiales.

EMI (*Electromagnetic Interference*, Interferencia electromagnética) y RFI (*Radio Frequency Interference*, Interferencia de frecuencia de radio) son dos consideraciones ambientales adicionales. Los motores, las luces y otros tipos de objetos electromecánicos provocan EMI, que pueden producir sobrecargas de circuitos, picos o fallos de los componentes eléctricos. Compruebe que todas las líneas de señal están protegidas y polarizadas correctamente para minimizar las interferencias EMI. Los dispositivos que las generan deberían estar físicamente separados del cableado tanto como sea posible porque este tipo de energía tiende a disiparse rápidamente con la distancia.

La figura 10.9 ilustra un motor generando EMI. En este ejemplo, el cable de datos que está al lado del motor está recogiendo las interferencias EMI. Esto provoca que la señal se deteriore y que pueda acabar causando la inutilidad de la línea. El área gris de la ilustración representa las interferencias generadas por el motor.

**********10_009.tif**********

<Pie figura>**Figura 10.9.** Interferencia electromagnética recogida con un cable de datos.

<Cuerpo texto>RFI es el subproducto de los proceso eléctricos, similar a EMI. La principal diferencia es que RFI suele proyectarse a través de un espectro de radio. Los motores con conexiones defectuosas pueden generar RFI, al igual que otra serie de dispositivos. Si los niveles de RFI son demasiado altos, podrían provocar que los receptores de unidades inalámbricas no detecten nada. Este proceso se llama insensibilización y se produce como consecuencia del volumen de energía RF. Esto puede ocurrir aunque las señales estén en distintas frecuencias.

La figura 10.10 muestra el proceso de insensibilización en un WAP (*Wireless Access Portal*, Portal de acceso inalámbrico). Las únicas soluciones en esta situación serían separar más los dispositivos o desactivar el generador RFI.

**********10_010.tif**********

<Pie figura>**Figura 10.10.** Insensibilización RF como resultado de interferencia de telefonía móvil.

<Cuerpo texto>En 1985, el investigador holandés Wim van Eck afirmaba que era posible curiosear en pantallas CRT (*Cathode Ray Tube*, Tubo de rayos catódicos) y LCD (*Liquid Crystal Display*, Pantalla de cristal líquido) detectando sus emisiones electromagnéticas. Conocido como Van Eck phreaking, este problema/posibilidad ha aparecido en las noticias recientemente debido a los posibles fallos con las máquinas de votación electrónica. TEMPEST recomienda algunas medidas defensivas para abordar este problema. Entre ellas que se incluye la protección.

**********INICIO DE NOTA**********

<Nivel 3>Proyecto TEMPEST

<Cuerpo texto>TEMPEST es el nombre de un proyecto iniciado por el gobierno de EE. UU. a finales de los años 50. Su objetivo era reducir el ruido electromagnético de dispositivos que divulgaban datos sobre los sistemas e información. Este programa se ha convertido en un estándar para la certificación de sistemas informáticos. La protección TEMPEST significa que un sistema informático no emite una cantidad importante de EMI o RFI. Para que un dispositivo se apruebe como TEMPEST, debe superar una comprobación exhaustiva, haciendo exactamente lo que determinan los estándares gubernamentales. Hoy en día, se utilizan zonas de control y ruidos de fondo para conseguir la protección. Los equipos con una certificación TEMPEST suelen costar dos veces más que los que no cuentan con este certificado.

**********FIN DE NOTA**********

<Nivel 2>Pasillos fríos y cálidos

<Cuerpo texto>En las habitaciones del servidor, suele haber varias filas de servidores colocadas en estantes. Estas se conocen como pasillos y pueden refrigerarse según sean fríos o cálidos. En el caso de un pasillo cálido, se utilizan

salidas de aire acondicionado para enfriar el equipo, mientras que en los pasillos fríos, se emplea una entrada de aire acondicionado para enfriarlo. Combinando los dos, tendrá entradas de aire frío abajo y salidas de aire caliente arriba, proporcionando una circulación constante.
Es importante que el aire caliente que ya está viciado procedente de un pasillo de estantes no sea el mismo que entre en el siguiente, si no se produciría un sobrecalentamiento. Los controladores del aire deben sacar el aire caliente mientras que el frío, que suele venir de una planta más alta, proporciona la entrada de aire. La figura 10.11 muestra un ejemplo del diseño de pasillos fríos y cálidos.
**********10_011.tif**********
<Pie figura>**Figura 10.11.** Ejemplo de diseño de pasillos fríos y cálidos.
<Nivel 1>Las medidas antiincendios
<Cuerpo texto>Las medidas antiincendios son una consideración clave en el diseño de centros informáticos. Este proceso se lleva a cabo para extinguir los incendios en lugar de prevenirlos. Dos de los principales tipos de sistemas antiincendios que se utilizan son: extintores y sistemas fijos.
<Nivel 2>Extintores
<Cuerpo texto>Los extintores son sistemas portátiles. Su selección y uso es de vital importancia. Hay básicamente cuatro tipos de extintores disponibles, clasificados por los tipos de incendio que apagan: A, B, C y D. La tabla 10.1 describe los cuatros tipos de incendios y las capacidades de los distintos extintores.
<Pie figura>**Tabla 10.1.** Clasificación de los extintores antiincendios.
<Tablas>

Tipo	**Uso**	**Composición del retardante**
A	Madera y papel	Básicamente agua o químicos
B	Líquidos inflamables	Químicos retardantes del fuego
C	Eléctricos	Químicos no conductivos
D	Metales inflamables	Varios, específico del tipo

<Nota>**Nota:** Existe un tipo de extintor K destinado al uso de incendios de aceites de cocina que también se puede adquirir. En la actualidad, hay un subconjunto de extintores de la clase B.
<Cuerpo texto>Muchos tipos de extintores con diferentes propósitos pueden combinar varias capacidades en una única botella. Los más comunes son AB, BC y ABC.
El procedimiento recomendado para utilizar un extintor antiincendios se conoce como método PASS (*Pull, Aim, Dqueeze, and Sweep*, Sacar, apuntar, apretar y barrer). Los extintores suelen funcionar solo unos segundos. Si utiliza uno, no se fije en un único punto. La mayoría tienen un rango limitado de efectividad, de tres a ocho metros.
<Nota>**Nota:** Algo primordial en el caso de los incendios eléctricos es que pueden reproducirse si no se corta la corriente. Compruebe que la desactiva cuando se produce un incendio.
<Cuerpo texto>Casi todos los extintores requieren de una inspección anual. Se trata de uno de los factores de revisión favoritos de los inspectores. Puede contratar servicios que lleven a cabo esta tarea y, así, inspeccionarán o sustituirán sus extintores según lo estipulado.
<Nivel 2>Sistemas fijos
<Cuerpo texto>Los sistemas fijos suelen formar parte de la infraestructura del edificio. Los más frecuentes combinan detectores de incendios con sistemas antiincendios. Los primeros suelen desencadenar los segundos debido a un rápido cambio en la temperatura o al exceso de humo. El sistema antiincendios utiliza aspersores de agua o gas antiincendios. En el caso de los aspersores, los sistemas de agua funcionan con salidas en la parte alta, como puede observar en la figura 10.12. Éstos son el método más utilizado en los edificios de nueva construcción. Los sistemas de agua son fiables, relativamente económicos y requieren poco mantenimiento.
**********10_012.tif**********
<Pie figura>**Figura 10.12.** Sistema antiincendios de agua.
<Cuerpo texto>El inconveniente de estos sistemas es que pueden provocar grandes daños en el equipo eléctrico, por ejemplo, en los ordenadores. Para evitarlo, pueden combinarse con transmisiones que desactiven la corriente de los sistemas informáticos antes de que se pongan en marcha los aspersores de agua en el edificio.
Los sistemas de gas se diseñaron originalmente para utilizar dióxido de carbono y, con posterioridad, gas halógeno. Este ya no se emplea porque daña la capa de ozono. No obstante, tiene a su disposición sustitutos que respetan el medio ambiente. Uno de los más comunes es el FM200. El principio de un sistema de gas es que desplaza el oxígeno de la habitación, eliminando uno de los componentes necesarios para un incendio.
<Nota>**Advertencia:** En caso de incendio, evacúe de forma inmediata la habitación. Los sistemas de gas funcionan eliminando el oxígeno y esto también podría asfixiar a alguien.
<Cuerpo texto>El principal inconveniente de los sistemas de gas es que requieren entornos precintados para funcionar. Por ello, se suelen instalar sistemas de ventilación especiales que limitan la circulación del aire cuando este se libera. Los sistemas de gas también son caros y, normalmente, solo se implementan en salas de informática u otras áreas en las que el agua podría dañar la tecnología u otra propiedad intelectual.
<Nivel 1>Resumen
<Cuerpo texto>En este capítulo, hemos tratado los elementos clave de la seguridad física y del entorno. Las medidas de seguridad física incluyen controles de acceso, barreras físicas y sistemas ambientales. Las consideraciones del entorno se refieren a cuestiones eléctricas, medidas antiincendios e interferencias.
Los modelos de seguridad se centran en la seguridad física, las zonas de seguridad, las particiones y la infraestructura de las comunicaciones. Debería adoptar un enfoque multidisciplinar cuando implemente un modelo de seguridad.
<Nivel 1>Ideas clave para el examen
<Cuerpo texto>A continuación, incluimos las ideas clave que debe recordar para el examen Security+:
<Sep-med>* **Aspectos de la seguridad física:** Esta se refiere a los mecanismos que pro`porcionan control de acceso, barreras físicas y sistemas de autenticación como la biometría.

* **Tipos de control de acceso utilizados en la seguridad física:** Los principales métodos de control de acceso incluyen la seguridad del perímetro, las zonas seguras, las barreras físicas y los sistemas de identificación. Cuando se implementan en capas es más difícil que acceda un intruso. Los métodos de acceso físico también deberían incluir sistemas para detectar intrusiones, por ejemplo, la vigilancia de vídeo para monitorizar las actividades cuando se produzcan. Esto ayuda a los profesionales de la seguridad a detectar la amenaza y realizar cambios cuando sea necesario.
* **Aspectos y funciones de los sistemas ambientales:** Incluyen la calefacción, el aire acondicionado, el control de la humedad, medidas antiincendios y los sistemas de energía. Todas estas funciones son críticas para el buen diseño de una planta.
* **Objetivos de la protección del entorno:** Principalmente, esta evita las interferencias de fuentes EMI y RFI. Se suelen colocar en zonas efectivas neutralizando o reduciendo la susceptibilidad a las interferencias.
* **Tipos de sistemas antiincendios que se utilizan hoy en día:** Pueden ser fijos o portátiles. Los sistemas portátiles suelen ser los extintores de incendios. Los fijos forman parte del edificio y pueden tener como elemento principal el agua o el gas. Los sistemas de gas solo se instalan en salas informáticas o en otras localizaciones en las que el agua causaría más daños que beneficios. Además, solo funcionan en entornos en que el flujo de aire sea limitado, ya que extraen el oxígeno del incendio y provocan su extinción. Los sistemas de agua suelen acabar con el calor de un incendio para extinguirlo.

<Nivel 1>Prueba de evaluación

<Sep-med>1. ¿Qué componente de la seguridad física se encarga del control de acceso de la capa externa?
A. Seguridad del perímetro. **B.** *Mantraps*. **C.** Zonas de seguridad. **D.** Puertas con candado.

2. Le han reclutado para el comité de seguridad. Una de sus primeras tareas es realizar el inventario de todos los extintores y comprobar que cada tipo está en el lugar adecuado del edificio. ¿Cuál de las siguientes categorías de extintores se utiliza para los incendios eléctricos?
A. Tipo A. **B.** Tipo B. **C.** Tipo C. **D.** Tipo D.

3. ¿Cuál de las siguientes opciones no reduce el EMI?
A. Protección física. **B.** Control de humedad. **C.** Localización física. **D.** Poner a punto los motores.

4. Es el administrador de una empresa. Está creando un equipo que le tenga al corriente de todo y está intentando dividir las responsabilidades entre los distintos miembros. De forma similar, ¿cuál de los siguientes métodos de acceso divide una zona grande en áreas más pequeñas para que puedan monitorizarse de forma individual?
A. Zona. **B.** Partición. **C.** Perímetro. **D.** Planta.

5. ¿Cuál de las siguientes opciones es el equivalente a construir tabiques en un edificio desde una perspectiva de red?
A. Seguridad del perímetro. **B.** Particiones. **C.** Zonas de seguridad. **D.** Sistemas IDS.

6. Tras una serie de pequeños incidentes, la seguridad física se ha convertido en una prioridad importante en su empresa. Ningún miembro del personal debería obtener acceso a los servidores o a los terminales sin autorización. ¿Cómo se llama el proceso para evitar el acceso a los sistemas informáticos de un edificio?
A. Seguridad del perímetro. **B.** Control de acceso. **C.** Zonas de seguridad. **D.** Sistemas IDS.

7. ¿Cuál de las siguientes opciones es un ejemplo de seguridad del perímetro?
A. Valla metálica. **B.** Videocámara. **C.** Ascensor. **D.** Sala informática cerrada con candado.

8. Es el jefe del comité de seguridad de una empresa. Tras un traslado a una nueva instalación, está implantando un nuevo sistema para controlar la seguridad. ¿Cuál de las siguientes opciones describe de forma más adecuada un detector de movimiento ubicado en una esquina del recibidor?
A. Seguridad del perímetro. **B.** Particiones. **C.** Zona de seguridad. **D.** Sistema IDS.

9. ¿Qué tecnología utiliza una característica física para establecer la identidad?
A. Biometría. **B.** Vigilancia. **C.** Tarjeta inteligente. **D.** Autenticador CHAP.

10. ¿Cómo se llama el proceso de reducir o eliminar la susceptibilidad a interferencias externas?
A. Protección. **B.** EMI. **C.** TEMPEST. **D.** Insensibilización.

11. Trabaja en una empresa de electrónica que acaba de crear un dispositivo que emite menos RF que el producto de la competencia. Dada la gran importancia de este invento y de los beneficios de marketing que podría ofrecer, quiere que el producto esté certificado. ¿Qué certificación se utiliza para indicar que las emisiones electrónicas son mínimas?
A. EMI. **B.** RFI. **C.** CC EAL 4. **D.** TEMPEST.

12. Debido al crecimiento de la capacidad actual, se está construyendo una nueva habitación de servidores. Como director, quiere comprobar que se instalan todos los elementos de seguridad necesarios al terminar. ¿Qué sistema de medidas antiincendios funciona mejor cuando se utiliza en un área aislada desplazando el aire del incendio?
A. De gas. **B.** De agua. **C.** Sistema fijo. **D.** Aspersores elevados.

13. El tipo K de los extintores es para incendios de aceite de cocina. Este tipo es un subconjunto de otro tipo de extintor, ¿de cuál?
A. Tipo A. **B.** Tipo B. **C.** Tipo C. **D.** Tipo D.

14. ¿Con cuál de las siguientes opciones funcionan los lectores de proximidad? (Hay varias opciones correctas.)
A. Tarjeta fob 15.75. **B.** Tarjeta de vigilancia 14.32. **C.** Tarjeta inteligente de 13.56 MHZ. **D.** Tarjeta de proximidad de 125 kHz.

15. En un sistema de pasillos fríos y cálidos, ¿cuál es el método habitual para gestionar el aire frío?
A. Bombear aire debajo del revestimiento del suelo. **B.** Bombear aire desde arriba del revestimiento del techo. **C.** Solo se extrae el aire caliente y el aire frío es el resultado natural. **D.** Hay aire frío en cada pasillo.

16. Si los niveles de RF son demasiado altos, pueden provocar que los receptores de las unidades inalámbricas no detecten nada. Este proceso se llama:
A. Recorte. **B.** Insensibilización. **C.** Distorsión. **D.** Chisporroteo.
17. RFI es el subproducto de un proceso eléctrico similar a EMI. La principal diferencia es que RFI está protegido mediante ¿cuál de las siguientes opciones?
A. Medio de red. **B.** Cableado eléctrico. **C.** Espectro de radio. **D.** Medios portátiles.
18. Para la seguridad física, ¿qué debería hacer con los servidores colocados en estantes?
A. Colocar un cable desde ellos hasta un escritorio. **B.** Colocar candados en el armario. **C.** Instalarlos en seguros. **D.** Utilizar solo tipo D, que incorpora su propia seguridad.
19. ¿Cuál de los siguientes es un método para enfriar los estantes de los servidores en los que el aire caliente y el frío se gestionan en la misma habitación de servidores?
A. Naves frías/calientes. **B.** Pasajes fríos/calientes. **C.** Pasarelas frías/calientes. **D.** Pasillos fríos y cálidos.
20. ¿Cuál de las siguientes es una instalación de alta seguridad que requiere identificación, así como autenticación, para obtener acceso?
A. *Mantrap*. **B.** Vallado. **C.** Lector de proximidad. **D.** Pasillo templado.
<Nivel 1>Respuestas de la prueba de evaluación
<Sep-med>1. A. La primera capa de control de acceso es la seguridad del perímetro. Está ideada para retrasar o impedir la entrada a una instalación.
2. C. El tipo C de extintores se utiliza para los incendios eléctricos.
3. B. Dispositivos eléctricos, como motores, que generan campos magnéticos provocan EMI. El control de la humedad no reduce el EMI.
4. A. La zona de seguridad es una parte más pequeña de un área más grande. Puede monitorizarse de forma individual si es necesario. Las respuestas B, C y D son ejemplos de zonas de seguridad.
5. B. La partición es el proceso que divide una red en componentes más pequeños que pueden protegerse de forma individual. Es el equivalente a construir tabiques en un edificio.
6. B. El control de acceso es el proceso principal para evitar el acceso a sistemas físicos.
7. A. La seguridad del perímetro implica crear un perímetro o frontera externa para un espacio físico. Los sistemas de vigilancia de vídeo no se consideran parte de la seguridad del perímetro pero pueden emplearse para mejorar el control de la seguridad física.
8. C. Una zona de seguridad es un área más pequeña de la instalación. Permite detectar intrusiones en partes específicas del edificio.
9. A. La biometría es una tecnología que utiliza una característica física para establecer la identidad, por ejemplo, patrones de retina o huellas.
10. A La protección evita que las señales electrónicas interrumpan las operaciones.
11. D. TEMPEST es la certificación que se da a los dispositivos electrónicos que emiten un mínimo de RF. Es difícil de adquirir e incrementa de forma significativa los costes de los sistemas.
12. A. Los sistemas de gas funcionan desplazando el aire del incendio. De este modo, se elimina uno de los tres componentes básicos de un incendio: el oxígeno.
13. B. El tipo K de extintores es un subconjunto del tipo B.
14. C, D. Los lectores de proximidad funcionan con tarjetas inteligentes de 13.56 MHZ y tarjetas de proximidad de 125 kHz.
15. A. Con los pasillos fríos y cálidos, el aire frío bombea aire debajo del revestimiento del suelo.
16. B. Si los niveles de RF son demasiado altos, pueden provocar que los receptores de las unidades inalámbricas no detecten nada. Este proceso se llama insensibilización y se produce debido al volumen de energía RF.
17. C. RFI es el subproducto de un proceso eléctrico similar a EMI. La principal diferencia es que RFI está protegido mediante un espectro de radio. Los motores con conexiones defectuosas pueden generar RFI, al igual que otra serie de dispositivos.
18. B. Los armarios *rack* bloquean los servidores que se instalan en éstos para evitar que alguien los coja y se lo lleve
19. D. Los pasillos fríos y cálidos son un método para enfriar los estantes de los servidores en los que el aire caliente y frío se gestionan en la misma habitación de servidores.
20. A. Las instalaciones de alta seguridad emplean un tipo de mecanismo de control de acceso intermedio conocido como *mantrap* (cepo), también se suele escribir como *man-trap*. Éstos requieren identificación visual y autenticación para obtener el acceso. Un *mantrap* hace que sea más difícil que varias personas accedan a la instalación porque solo permite que entren uno o dos individuos al mismo tiempo.

Capítulo 12. Seguridad de red inalámbrica

<Cuerpo texto>En este capítulo se tratan los siguientes objetivos del examen CompTIA Security+:
<Sep-med>1.6 Implementar una red inalámbrica de modo seguro.
3.4 Analizar y diferenciar entre los tipos de ataque inalámbricos.
<Cuerpo texto>En resumidas cuentas, los sistemas inalámbricos son sistemas que no utilizan cables para enviar información sino que transmiten los datos a través del aire. El crecimiento de este tipo de sistemas crea muchas oportunidades para los atacantes. Se trata de una tecnología relativamente nueva, utiliza mecanismos de comunicaciones bien establecidas y son fáciles de interceptar.
Este capítulo se centra en los distintos tipos de sistemas inalámbricos que puede encontrar y menciona algunas de las cuestiones de seguridad asociadas a esta tecnología. En concreto, los sistemas trabajan con WTLS (*Wireless Transport Layer Security*, Seguridad para la capa de transporte en comunicaciones inalámbricas), estándares inalámbricos IEEE 802, WPA2, aplicaciones WEP/WAP y con las vulnerabilidades que presentan cada uno de ellos.
<Nivel 1>Trabajar con sistemas inalámbricos
<Cuerpo texto>Los días del cable coaxial recorriendo las habitaciones pertenecen al pasado. Cada vez más, nos estamos trasladando a un entorno en el que las redes inalámbricas son la topología elegida. Para conseguir que este entorno sea adecuado y aprobar el examen de CompTIA, es necesario que entienda los estándares 802.11 aplicables, así como las tecnologías (las implementaciones de los estándares) que se utilizan actualmente.
Esta sección se centra en los protocolos que debe conocer, así como en la implementación de la capa de transporte.
<Nivel 2>Protocolos inalámbricos IEEE 802.11x
<Cuerpo texto>La familia de protocolos IEEE 802.11x proporciona comunicaciones inalámbricas utilizando transmisiones de frecuencia de radio. Las frecuencias que emplean los estándares 802.11 son el espectro de 2.4GHz y 5GHz. Se han definido anchos de banda para entornos inalámbricos y, a excepción de 802.11a, suelen ser compatibles entre sí.
<Sep-med>* **802.11:** Este estándar define las LAN inalámbricas que se transmiten en anchos de banda de 1Mbps o 2Mbps empleando el espectro de frecuencia 2.4GHz y utilizando FHSS (*Frequency-Hopping Spread Spectrum*, Espectro ensanchado por salto de frecuencia) o DSSS (*Direct-Sequence Spread Spectrum*, Espectro ensanchado por secuencia directa) para codificar los datos.
* **802.11a:** Este estándar proporciona ancho de banda para redes inalámbricas LAN de hasta 54 Mbps en el espectro de frecuencia de 5GHz. Además, utiliza OFDM (*Orthogonal Frequency Division Multiplexing*, Multiplexación por división de frecuencias ortogonales) para la codificación en lugar de FHSS o DSSS.
* **802.11b:** Este estándar proporciona ancho de banda de hasta 11 Mbps (con índices de reserva de 5.5, 2 y 1 Mbps) en el espectro de frecuencia de 2.4GHz. También se conoce como Wi-Fi o 802.11 de alta frecuencia. El estándar 802.11b solo utiliza DSSS para codificar los datos.
* **802.11g:** Este estándar proporciona ancho de banda de hasta 54 Mbps en el espectro de frecuencia de 2.4GHz. Aunque puede obtener velocidades más rápidas, también sufre de los mismos problemas de interferencia inherentes a 802.11b, tener que compartir el espectro con otros dispositivos que utilizan esa frecuencia.
* **802.11i:** Este proporciona mejoras de seguridad para el estándar inalámbrico con especial atención a la autenticación. Se suele conocer como WPA2, el nombre que le dio la alianza Wi-Fi.
* **802.11n:** Este estándar proporciona ancho de banda de hasta 300 Mbps en el espectro de frecuencia de 5GHz (también puede comunicarse en 2.4GHz por cuestiones de compatibilidad). La ventaja de este estándar es que ofrece alta velocidad y una frecuencia que no tiene muchas interferencias.
<Cuerpo texto>En la mayoría de ocasiones, un punto de acceso inalámbrico funciona con más de un estándar 802.11. En la figura 12.1, por ejemplo, Dell Wireless WLAN Card Utility (utilidad de la tarjeta Dell de red WLAN inalámbrica) muestra que la mayoría de redes que puede detectar utilizan 802.11b, 802.11g y 802.11n.
**********12_001.tif**********
<Pie figura>**Figura 12.1.** La mayoría de las redes inalámbricas detectadas utilizan más de un estándar 802.11.
<Cuerpo texto>Se utilizan tres tecnologías para comunicarse en el estándar 802.11 y proporcionan compatibilidad retroactiva con 802.11b:
<Sep-med>* **DSSS (*Direct-Sequence Spread Spectrum*, Espectro ensanchado por secuencia directa):** Hace posible la comunicación añadiendo los datos que se transfieren a transmisiones de una velocidad superior. Esta contiene información redundante para asegurar la precisión de los datos. Cada paquete puede reconstruirse en caso de que se produzca alguna interrupción.
* **FHSS (*Frequency-Hopping Spread Spectrum*, Espectro ensanchado por salto de frecuencia):** Hace posible la comunicación mediante un salto de transmisión sobre un rango de frecuencias predefinidas. El cambio o salto se sincroniza entre ambos extremos y parece ser un único canal de transmisión para ellos.
* **OFDM (*Orthogonal Frequency Division Multiplexing*, Multiplexación por división de frecuencias ortogonales):** Hace posible la comunicación descomponiendo los datos en señales secundarias y las transmite de forma simultánea. Estas transmisiones se producen en distintas frecuencias o bandas subordinadas.
<Cuerpo texto>Los procesos matemáticos y las teorías de estas tecnologías de transmisión están más allá del ámbito de este libro.
<Nivel 2>WEP/WAP/WPA/WPA2
<Cuerpo texto>WEP (*Wired Equivalent Privacy*, Privacidad equivalente a cableado) se creó para proporcionar una seguridad básica para las redes inalámbricas, aunque este tipo de sistemas suelen utilizar WAP (*Wireless Application Protocol*, Protocolo de aplicaciones inalámbricas) para las comunicaciones de red. Con el tiempo, WEP ha ido

sustituyendo a WPA y WPA2 en la mayoría de implementaciones. Las siguientes secciones describen brevemente estos términos y facilitan el entendimiento de sus respectivas capacidades.
<Nivel 3>Privacidad equivalente a cableado
<Cuerpo texto>WEP (*Wired Equivalent Privacy*, Privacidad equivalente a cableado) es un protocolo inalámbrico que proporciona el equivalente de privacidad a una red inalámbrica. WEP se implementa en algunos dispositivos inalámbricos, incluyendo los PDA y los teléfonos móviles. Este es vulnerable debido a las debilidades en el modo de empleo de los algoritmos de cifrado (RC4). Estas vulnerabilidades permiten que el algoritmo se pueda descifrar en unos cinco minutos utilizando el software de ordenador disponible. Esto hace que WEP sea uno de los protocolos más vulnerables en términos de seguridad.
Por ejemplo, el IV (*Initialization Vector*, Vector de inicialización) que utiliza WEP para el cifrado es de 24 bit, que es bastante débil y significa que los IV se reutilizan con la misma clave. Examinando el resultado repetitivo, es fácil que alguien descifre la clave secreta WEP. Esto se conoce como ataque IV. Para coger algo de perspectiva, sepa que el ataque se produce porque el algoritmo utilizado es RC4, el IV es demasiado pequeño, estático y forma parte de la clave de cifrado RC4.
La figura 12.2 muestra los ajustes de configuración del enrutador de una red inalámbrica simple y resume la mejor situación: En la única ocasión que se utiliza WEP es cuando debe tener compatibilidad con dispositivos más antiguos que no admiten nuevo cifrado.
**********12_002.tif**********
<Pie figura>**Figura 12.2.** Ajustes de seguridad inalámbrica para un enrutador simple.
<Cuerpo texto>Para hacer que el cifrado sea más fuerte, se empleaba TKIP (*Temporal Key Integrity Protocol*, Protocolo temporal de integridad de clave). Este coloca un contenedor de 128 bits alrededor del cifrado WEP con una clave basada en elementos como la dirección MAC de su máquina y el número de serie del paquete. TKIP se diseñó como un sustituto compatible con versiones anteriores para WEP y podría utilizar todo el hardware existente. Sin el uso de TKIP, WEP, como mencionamos anteriormente, se considera débil. Sin embargo, tenga en cuenta que incluso TKIP ha sido descifrado.
<Nivel 3>Protocolo de aplicaciones inalámbricas
<Cuerpo texto>WAP (*Wireless Application Protocol*, Protocolo de aplicaciones inalámbricas) es la tecnología diseñada para los dispositivos inalámbricos. Se ha convertido en el estándar adoptado por muchos fabricantes, incluyendo a Motorola y Nokia. Las funciones WAP son equivalentes a TCP/IP, ya que intentan servir al mismo propósito para los dispositivos inalámbricos. WAP utiliza una versión más pequeña de HTML llamada WML (*Wireless Markup Language*, Lenguaje de marcado inalámbrico), que se utiliza para presentaciones de Internet. Los dispositivos con WAP habilitado también pueden responder a secuencias de comandos utilizando un entorno llamado WMLScript. Este es similar a Java, un conocido lenguaje de programación.
La habilidad de aceptar páginas Web y secuencias de comandos produce la oportunidad de que el código malicioso y los virus se transporten para dispositivos con WAP habilitada. La habilidad de aceptar páginas Web y secuencias de comandos crea la oportunidad de que código malicioso o virus se transporten a dispositivos con WAP habilitado. No cabe ninguna duda de que esto conlleva algunos problemas y necesitará software antivirus para solucionarlos.
Los sistemas WAP se comunican utilizando una puerta de enlace WAP, como puede observar en la figura 12.3. Esta convierte la información de HTTP a WAP y viceversa. Además, también codifica y decodifica la información entre ambos protocolos.
**********12_003.tif**********
<Pie figura>**Figura 12.3.** Una puerta de enlace WAP habilita una conexión para los dispositivos WAP a través de Internet.
<Cuerpo texto>Esta estructura proporciona unas garantías razonables de que los dispositivos habilitados para WAP son seguros. Si la interconexión entre el servidor WAP e Internet no está cifrada, podrán interceptarse los paquetes entre ambos dispositivos (esto se conoce como husmear paquetes), creando una posible vulnerabilidad. Esta se llama hueco en el WAP (tenía lugar al convertir entre WAP y SSL/TLS) y era muy frecuente en versiones anteriores a 2.0.
<Nivel 3>Acceso Protegido Wi-Fi y WPA2
<Cuerpo texto>Las tecnologías WPA (*Wi-Fi Protected Access*, Acceso Protegido Wi-Fi) están diseñadas para tratar los problemas básicos de WEP. Se crearon para implementar el estándar 802.11i. La diferencia entre WPA y WPA2 es que el primero implementa la mayoría, pero no todos, los 802.11i para poder comunicarse con tarjetas inalámbricas más antiguas (puede que aun así tenga que actualizar su firmware para que sea compatible) y utiliza el algoritmo de cifrado RC4 con TKIP, mientras que WPA2 implementa el estándar completo y no es compatible con tarjetas más antiguas.
WPA también exige el uso de TKIP y WPA2 aboga por CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*, Cifrado de bloques en cadena y autenticación del mensaje). Este utiliza un cifrado AES de 128-bits con un vector de inicialización. Cuanto mayor sea este, mayor será la dificultad para descifrarlo y minimiza el riesgo de reproducción.
Para el examen, piense que WEP es anterior. Este estaba plagado de errores y WPA (con TKIP) se empleó como solución intermedia, implementando una parte del estándar 802.11i. La solución final es WPA2 (con CCMP), una implementación completa del estándar 802.11i.
<Nivel 2>Seguridad para la capa de transporte en comunicaciones inalámbricas
<Cuerpo texto>WTLS (*Wireless Transport Layer Security*, Seguridad para la capa de transporte en comunicaciones inalámbricas) es la capa de transporte del protocolo de aplicación inalámbrica, que tratamos anteriormente. Este proporciona autenticación, cifrado e integridad de datos para los dispositivos inalámbricos. Se diseñó para utilizar el relativamente estrecho ancho de banda de este tipo de dispositivos y es bastante seguro. WTLS proporciona una seguridad razonable para dispositivos móviles y se está implementando en dispositivos inalámbricos.

La seguridad para la capa de transporte en comunicaciones inalámbricas proporciona una conexión cifrada y autenticada entre un cliente inalámbrico y un servidor. WTLS es similar en su función a TLS, pero utiliza un ancho de banda más bajo y menos energía de procesamiento. Se utiliza para prestar soporte a dispositivos inalámbricos, que todavía no tienen procesadores con la suficiente energía.
La figura 12.4 ilustra WTLS como parte del entorno WAP. Este proporciona el equivalente de funcionalidad de TCP/IP para dispositivos inalámbricos. Muchos dispositivos, incluyendo los teléfonos móviles más recientes y los PDA, son compatibles con WTLS como parte de sus capacidades de protocolo de red.
**********12_004.tif**********
<Pie figura>**Figura 12.4.** Uso de WTLS entre dos dispositivos WAP.
<Nota>**Truco:** La comunicación entre un auricular WAP y el servidor WAP está protegida por WTLS. Una vez en Internet, una conexión suele estar protegida por SSL (*Secure Socket Layer*, Protocolo de capa de conexión segura), un estándar de Internet para cifrar datos entre puntos de la red.
<Nivel 1>Dispositivos móviles
<Cuerpo texto>Los dispositivos móviles, incluyendo smartphones, e-readers, tablets y PDA (*Personal Digital Assistants*, Asistente digital personal), son muy populares. Muchos de estos dispositivos utilizan señales RF o tecnologías móviles para la comunicación. La figura 12.5, por ejemplo, muestra un Amazon Kindle para redes inalámbricas.
**********12_005.tif**********
<Pie figura>**Figura 12.5.** El escaneo inalámbrico se realiza en una gran variedad de dispositivos como Kindle.
<Cuerpo texto>Si el dispositivo utiliza WAP (*Wireless Application Protocol*, Protocolo de aplicaciones inalámbricas), es probable que no tenga seguridad habilitada. Existen muchos niveles de seguridad en WAP:
<Sep-med>* **Autenticación anónima:** Permite que prácticamente todo el mundo se conecte al portal inalámbrico.
* **Autenticación del servidor:** Requiere que el terminal se autentique frente al servidor.
* **Autenticación de dos vías (cliente y servidor):** Requiere que se autentiquen los dos extremos de la conexión para confirmar la validez.
<Cuerpo texto>Muchos de los nuevos dispositivos también pueden utilizar certificados para verificar la autenticación. La figura 12.6 muestra una red de sistemas móviles, esta red utiliza tanto el cifrado como la autenticación para incrementar la seguridad.
**********12_006.tif**********
<Pie figura>**Figura 12.6.** Entorno móvil utilizando una seguridad WAP.
<Cuerpo texto>Las siguientes tecnologías se utilizan para proporcionar servicios entre los dispositivos:
<Sep-med>* **WSP (*Wireless Session Protocol*, Protocolo de sesión inalámbrica):** Gestiona la información de sesión y la conexión entre los dispositivos.
* **WTP (*Wireless Transaction Protocol*, Protocolo de transacción inalámbrica):** Proporciona servicios similares a TCP y UDP para WAP.
* **WDP (*Wireless Datagram Protocol*, Protocolo de datagrama inalámbrico):** Proporciona la interfaz común entre los dispositivos.
* **WTLS (Wireless Transport Layer Security, Seguridad para la capa de transporte en comunicaciones inalámbricas):** Es la capa de seguridad del protocolo de aplicación inalámbrica.
<Nivel 2>Puntos de acceso inalámbrico
<Cuerpo texto>No es muy complicado crear una red inalámbrica. En el lado del cliente, necesita una NIC (*Network Interface Card*, Tarjeta de interfaz de red) inalámbrica en lugar una NIC estándar de cableado. En el lado de la red, necesita algo para comunicarse con los clientes.
El principal método para conectar un dispositivo inalámbrico a una red es a través de un portal inalámbrico. Un punto de acceso inalámbrico (normalmente conocido como punto de acceso o PA) es un receptor/transmisor de baja energía, también llamado transceptor, que se coloca de forma estratégica para el acceso. El dispositivo inalámbrico y el punto de acceso se comunican utilizando varios protocolos de comunicación, incluyendo IEEE 802.11 (también conocido como Wi-Fi).
Como su nombre implica, las comunicaciones inalámbricas no utilizan el cableado como base de la comunicación. En la mayoría de ocasiones, utilizan una porción del espectro de frecuencia de radio (FR) llamado microondas. Los métodos de comunicación inalámbricas se están convirtiendo en los más utilizados en informática porque el coste del equipo de transmisión y recepción han descendido drásticamente en los últimos años. Las redes inalámbricas también ofrecen conectividad dentro de un campus, un edificio o incluso una ciudad. La mayoría de frecuencias inalámbricas compartidas por más de una persona pueden emplear la misma frecuencia para la comunicación.
La figura 12.7 ilustra un portal inalámbrico utilizado para conectar un ordenador a una red de empresa. Observe que el portal se conecta a la red y se trata como cualquier otra conexión utilizada en la red.
**********12_007.tif**********
<Pie figura>**Figura 12.7.** Portal de acceso inalámbrico y el terminal.
<Cuerpo texto>Comunicaciones inalámbricas, aunque muy prácticas, puede ser menos que seguro. Aunque muchos PA ahora tienen cifrado activado, aun así querrá verificar que es el caso de su red. En la figura 12.1, es posible ver que no se utiliza seguridad. La figura 12.8 muestra un paquete procedente de una red insegura, mientras que la figura 12.9 ilustra la información procedente de una red habilitada. Observa la lista de protocolos en la mitad inferior de la figura 12.9.
**********12_008.tif**********
<Pie figura>**Figura 12.8.** Datos de una red insegura.
**********12_009.tif**********

<Pie figura>**Figura 12.9.** Datos de una red segura.
<Nivel 3>Colocación de la antena
<Cuerpo texto>La colocación de la antena puede ser crucial para permitir que los clientes alcancen el punto de acceso. No hay una solución universal para esta cuestión, ya que depende del entorno en el que se coloca el punto de acceso. Como regla general, cuanta mayor distancia deba recorrer la señal, más se atenuará esta, pero puede perder una señal rápidamente en un breve espacio si los materiales del edificio la reflejan o absorben. Debería intentar evitar colocar los puntos de acceso cerca de metal (que incluye aparatos) o del suelo. En el centro del área se recomienda colocarla lo bastante arriba para sobrepasar la mayoría de los obstáculos. En el caso de que la señal viaje demasiado lejos, algunos puntos de acceso incluyen controles de nivel de energía que le permiten reducir la cantidad de salida que se proporciona.
**********INICIO DE NOTA**********
<Nivel 3>Calcular la fuerza de la señal
<Nota>Uno de los aspectos más problemáticos de las redes inalámbricas es intentar calcular la potencia de la señal entre el PA y los clientes. Se suele bromear con que un hacker que está fuera del edificio puede acceder a la red pero un usuario que está dentro no obtiene una señal lo bastante fuerte como para estar conectado en la red.
Piense en la señal en términos de cualquier otra señal de radio. Su fuerza se reduce considerablemente si está bloqueada por tabiques, armarios de metal u otras barreras. La señal puede traspasar ventanas de cristal y tabiques delgados sin dificultad.
Cuando está fuera de una red, es muy recomendable que instale un medidor de intensidad de señal en un terminal, hay muchos que puede descargar gratuitamente, y utilizarla para evaluar la fuerza de la señal que está recibiendo. Si la seña es débil, puede añadir PA adicionales y repetidores en la red, igual que si estuviera en una red de cableado.
**********FIN DE NOTA**********
<Nota>**Nota:** Puede encontrar una gran fuente de información sobre valores de energía RF y antena en el sitio Web de Cisco: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00800e90fe.shtml.
<Nivel 3>Filtrado MAC
<Cuerpo texto>La mayoría de los PA ofrecen la posibilidad de activar el filtrado MAC, pero está desactivada de forma predeterminada. La dirección MAC es el único identificador que existe para cada tarjeta de red (una parte de la dirección hexadecimal identifica al fabricante y la otra actúa como número de serie). En la fase predeterminada, cualquier cliente inalámbrico que conozca los valores requeridos puede unirse a la red. Cuando se utiliza el filtrado MAC, el administrador compila una lista de direcciones MAC asociada con los ordenadores de los usuarios y los introduce. Cuando un cliente intenta conectarse y se han introducido otros valores correctamente, se lleva a cabo una comprobación adicional de la dirección MAC. Si esta aparece en la lista, se permite acceder al cliente. De lo contrario, se le prohibirá el acceso. En algunos dispositivos inalámbricos, se utiliza el término bloqueo de red en lugar de filtrado MAC y los dos son sinónimos.
<Nota>**Nota:** La debilidad del filtrado MAC es que la dirección MAC es un valor que alguien con malas intenciones podría suplantarla para conseguir entrar. Haciendo pensar que su host ilegítimo es legítimo, pasará el filtro y obtendrá acceso.
<Cuerpo texto>En el ejercicio 12.1 aprenderá a modificar el orden de las redes favoritas en Windows Vista. Estas se limitan en Windows 7 y Windows Vista a las redes a las que se ha conectado con éxito.
**********Inicio ejercicio**********
<Nivel 4>Ejercicio 12.1. Cambiar el orden de las redes favoritas
<Cuerpo texto>La mayoría de clientes inalámbricos pueden recibir señales desde más de una red inalámbrica y conectarse a una de ellas. Si una red inalámbrica no está disponible, la conexión se realizará a través de la siguiente en la lista. Por esta razón, es importante que las redes inalámbricas estén en el orden que quiere para intentar la conexión. El siguiente ejercicio podrá modificar este orden:
<Sep-med>1. En un cliente Windows Vista, haga clic en el botón **Windows**, escriba **Centro de redes y recursos compartidos** en el cuadro **Buscar** y pulse **Intro**.
**********12_010.tif**********
<Pie figura>**Figura 12.10.** Centro de redes y recursos compartidos.
<Sep-med>2. Seleccione **Administrar redes inalámbricas** (véase la figura 12.11).
**********12_011.tif**********
<Pie figura>**Figura 12.11.** Administrar redes inalámbricas.
<Sep-med>3. Haga clic en una de las redes que aparezcan en la lista y arrástrela hacia arriba o hacia abajo para cambiar el orden de las redes favoritas.
4. Salga de **Administrar redes inalámbricas**.
5. Salga de **Centro de redes y recursos compartidos**.
**********Fin ejercicio**********
<Nivel 2>Protocolo de autenticación extensible
<Cuerpo texto>EAP (*Extensible Authentication Protocol*, Protocolo de autenticación extensible) proporciona un marco para la autenticación que se suele utilizar con redes inalámbricas. Entre los cinco tipos de EAP adoptados por el estándar WPA/WPA2 son EAP-TLS, EAP-PSK, EAP-MD5 y dos que necesitará conocer para el examen: LEAP y PEAP. La figura 12.11 muestra la información de configuración en una tarjeta WLAN que utiliza EAP-TTLS. Esta es una forma de EAP-TLS que añade túnel (Protocolo de autenticación extensible y Seguridad de capa de transporte con túnel).
**********12_012.tif**********
<Pie figura>**Figura 12.12.** Utilizar EAP-TTLS en una red inalámbrica.

<Cuerpo texto>Añadiendo en túnel, TTLS añade una capa más de seguridad frente a ataques hombre en el medio o el espionaje.
<Nivel 2>Protocolo de autenticación extensible ligero
<Cuerpo texto>Cisco creó LEAP (*Lightweight Extensible Authentication Protocol*, Protocolo de autenticación extensible ligero) como una extensión de EAP (*Extensible Authentication Protocol*, Protocolo de autenticación extensible) pero se ha ido retirando paulatinamente a favor de PEAP. Debido a que es propiedad de Cisco y solo se creó para resolver rápidamente problemas de WEP, no es compatible con Windows.
LEAP requiere autenticación mutua para mejorar la seguridad pero es susceptible de ataques de diccionario. EAP se considera un protocolo débil y, actualmente, Cisco no recomienda su uso.
<Nota>**Nota:** Puede encontrar bibliografía sobre seguridad inalámbrica LAN de Cisco que describe la arquitectura LEAP en http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_white_paper09186a00800b469f_ps4570_Products_White_Paper.html.
<Nivel 2>Protocolo de autenticación extensible protegido
<Cuerpo texto>Cisco, RSA y Microsoft crearon PEAP (*Protected Extensible Authentication Protocol*, Protocolo de autenticación extensible protegido). Este sustituye a LEAP y es compatible con Windows (que anteriormente abogaba por EAP-TLS) empezando por Windows XP. Hay compatibilidad con todos los sistemas operativos de Windows desde entonces, incluyendo Windows Vista y Windows 7.
Aunque muchos consideran que PEAP y EAP-TTLS son opciones similares, PEAP es más seguro porque establece un canal cifrado entre el servidor y el cliente.
<Nota>**Nota:** Puede encontrar bibliografía sobre seguridad inalámbrica LAN de Cisco que describe la arquitectura PEAP en http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_white_paper09186a00800b469f_ps4570_Products_White_Paper.html.
<Nivel 1>Vulnerabilidades inalámbricas
<Cuerpo texto>Los sistemas inalámbricos son vulnerables a la misma variedad de ataques que las redes de cableado. Sin embargo, debido a que estos protocolos utilizan señales de frecuencia de radio para la emanación de datos, tienen una debilidad adicional: estas pueden interceptarse con gran rapidez. Para interceptar tráfico 802.11x, todo lo que necesita es un ordenador que tenga instalada la tarjeta 802.11x adecuada. Muchas redes difunden con regularidad su nombre (conocido como transmisión SSID) para anunciar su presencia. El software simple en el ordenador puede capturar el tráfico de enlace en el PA inalámbrico y, a continuación, procesa estos datos para descifrar la información sobre la cuenta y la contraseña.
<Nota>**Nota:** Un método para proteger la red que se suele recomendar muy a menudo es desactivar la difusión SSID. El punto de acceso sigue estando ahí y los que lo conocen pueden acceder a él pero, de este modo, evita que alguien lo encuentre al realizar un escaneo. Este debería considerarse una forma muy débil de seguridad ya que hay otras formas para descubrir la presencia del punto de acceso, aunque un poco más complicadas, aparte de la difusión SSID.
<Cuerpo texto>En el ejercicio 12.2 aprenderá cómo configurar Windows Vista para conectar una red para desactivar la transmisión SSID.
**********Inicio ejercicio**********
<Nivel 4>Ejercicio 12.2. Configurar una conexión inalámbrica para la no difusión
<Cuerpo texto>Si quiere configurar el cliente de una red aunque no tenga activada la difusión SSID, siga estos pasos:
<Sep-med>1. En un cliente Windows Vista, haga clic con el botón derecho del ratón sobre el icono de una red y seleccione **Conectarse a una red** (véase la figura 12.13).
**********12_013.tif**********
<Pie figura>**Figura 12.13.** Conectarse a una red.
<Sep-med>2. Haga clic con el botón derecho del ratón sobre el icono de la red a la que está conectado y seleccione **Propiedades** (véase la figura 12.14).
**********12_014.tif**********
<Pie figura>**Figura 12.14.** Ventana Propiedades.
<Sep-med>3. Seleccione la ficha **Conexión** y active la casilla de verificación **Conectarse aunque la red no sea de difusión** (véase la figura 12.15).
**********12_015.tif**********
<Pie figura>**Figura 12.15.** Ventana Conexión.
<Sep-med>4. Haga clic en **Aceptar**.
5. Cierre el cuadro de diálogo **Conectarse a una red**.
**********Fin ejercicio**********
<Cuerpo texto>Un aspecto adicional de los sistemas inalámbricos es el sondeo del sitio. Este implica escuchar en una red inalámbrica existente utilizando tecnologías disponibles en el mercado. Esto le permite capturar información y datos, para que funcionen en sistemas de su red inalámbrica.
En un principio, el término sondeo del sitio significaba determinar si una localización dada estaba libre de interferencias. Cuando lo emplea un atacante, puede indicar qué tipos de sistemas están en uso, los protocolos empleados y otra información crítica sobre su red. Este es el método principal que se utiliza para recopilar datos sobre las redes inalámbricas. Casi todas ellas son vulnerables al sondeo del sitio.
Si se instalan portales inalámbricos en un edificio, las señales pueden llegar más allá del interior del edificio y pueden detectarse y decodificarse fuera de este utilizando un equipo nada caro. El término *wardriving* se refiere a rastrear una ciudad con un ordenador portátil buscando puntos de acceso inalámbricos para comunicarse con ellos. Su tarjeta de

red está configurada en modo promiscuo y busca señales procedentes de cualquier parte. Cuando los intrusos obtengan el acceso, puede robar conexión a Internet o corromper sus datos.
Una vez que se ha descubierto debilidad en una red, se puede producir *warchalking* (CompTIA se refiere a él como *war chalking*). Esto implica que los que descubran un modo de dejar señales de red (a menudo las escriben con tiza) o, en el exterior, la premisa para notificar a otros que la vulnerabilidad está ahí. Las marcas pueden estar en la acera, al lado del edificio, un poste cercano, por ejemplo, o todo lo que recuerde a los símbolos que aparecen en la figura 12.15. La figura 12.6 ilustra un ejemplo de lo que incluiría un nodo abierto.
**********12_015.tif**********
<Pie figura>**Figura 12.15.** Los símbolos de warchalking.
**********12_016.tif**********
<Pie figura>**Figura 12.16.** Ejemplo de símbolo de nodo abierto.
<Cuerpo texto>El cifrado débil era una cuestión a tener en cuenta en los puntos de acceso anteriores, pero gran parte de los controladores inalámbricos más recientes utilizan SSID (*Special ID Numbers*, Números especiales de ID) y deben configurarse en las tarjetas de red para hacer posibles las conexiones. Sin embargo, utilizar configuraciones de números ID no evita necesariamente que se monitoricen las redes inalámbricas. Por ejemplo, una organización maliciosa podría aprovecharse de los puntos de acceso inalámbricos no autorizados. Cualquier punto de acceso que no se haya autorizado se considera un *rogue*.
Un atacante o un usuario inocente que quiera mejorar su entorno podrían añadir un punto de acceso no autorizado. El problema con el usuario sería que al hacer esto es muy probable que no implemente seguridad y podría abrir el sistema a un ataque hombre en el medio o gemelo diabólico. En este último, punto de acceso inalámbrico no autorizado se hace pasar por proveedor de servicio inalámbrico legítimo para interceptar la información que transmiten los usuarios.
Eduque y forme a los usuarios sobre las redes inalámbricas y la necesidad de que estas sean seguras de igual modo que lo hace con otros temas relacionados con la seguridad. Puede que ellos piensen que no corren ningún peligro al conectarse a cualquier red inalámbrica que encuentren cuando viajen, como las que aparecen en la figura 12.17, pero deberían preguntarse si los administradores de otras redes tienen las mejores intenciones con respecto a los datos de su empresa en realidad.
**********12_017.tif**********
<Pie figura>**Figura 12.17.** Ejemplo de algunas redes inalámbricas cuestionables disponibles para la conexión.
<Cuerpo texto>No olvide cambiar la configuración predeterminada de todos los dispositivos inalámbricos. Nunca debe dar por hecho que las conexiones inalámbricas son seguras. Las emisiones de los portales pueden detectarse a través de las paredes y de varios bloques. La intercepción es fácil de llevar a cabo, dado que RF es el medio que se utiliza para la comunicación. Los dispositivos inalámbricos más recientes ofrecen seguridad de datos y debería emplearla. Puede configurar los PA y los enrutadores inalámbricos más modernos para la no difusión además de establecer un nivel de cifrado WPA2 y superior.
Con la creciente popularidad de Bluetooth, se han añadido dos vulnerabilidades: *bluejacking* y *bluesnarfing*. El primero consiste en enviar mensajes no solicitados (por ejemplo, el spam) mediante una conexión Bluetooth. Aunque molesto, no se considera muy dañino. El Bluetooth se suele utilizar para crear PAN (*Personal Area Networks*, Redes de área personal) y gran parte de estos dispositivos incorpora un PIN de fábrica predeterminada que debería modificar para establecer valores más seguros.
Bluesnarfing es obtener acceso no autorizado a través de una conexión Bluetooth. Este puede conseguirse a través de un teléfono, una PDA o cualquier otro dispositivo que utilice Bluetooth. Una vez que haya accedido, el atacante puede copiar todos los datos del mismo modo que cualquier otro acceso no autorizado.
<Nota>**Nota:** El estándar Bluetooth ha considerado las debilidades de esta tecnología y cada vez es más seguro. Una de las maneras más simples para asegurar dispositivos Bluetooth es no establecer su atributo como Reconocible.
<Nivel 1>Resumen
<Cuerpo texto>La popularidad y la estandarización de los sistemas inalámbricos está creciendo cada vez más. El protocolo que se implementa con más frecuencia es WAP. Su capa de seguridad es WTLS. WAP es equivalente a TCP/IP para los sistemas inalámbricos.
IEEE desarrolla los estándares para los sistemas inalámbricos. Los más comunes son 802.11, 802.11a, 802.11b, 802.11i, 802.11g y 802.11n. Estos estándares utilizan el espectro de frecuencia de 2.4GHz o 5GHz a excepción de 802.11i que es un estándar de seguridad que se suele conocer como WPA2. Hay muchas tecnologías de comunicación disponibles para enviar mensajes entre los dispositivos inalámbricos.
Las redes inalámbricas son vulnerables a los sondeos del sitio. Éstos pueden llevarse a cabo utilizando un ordenador y una tarjeta 802.11x. El término sondeo del sitio también hace referencia a detectar interferencias en un área dada que puede impedir que 802.11x funcione.
Hay varios estándares de seguridad para las redes inalámbricas. WEP (*Wired Equivalent Privacy*, Privacidad Equivalente a Cableado) era el más utilizado. Este estaba plagado de errores y WPA (con TKIP) se empleó como solución intermedia, implementando una parte del estándar 802.11i. La solución final es WPA2 (con CCMP), una implementación completa del estándar 802.11i.
Las vulnerabilidades existen debido a las debilidades de los protocolos. Por ejemplo, WEP es vulnerable a causa del empleo de algoritmos de cifrado. El IV (*Initialization Vector*, Vector de inicialización) que utiliza WEP para el cifrado es de 24 bit, que es bastante débil y significa que los IV se reutilizan con la misma clave. Examinando el resultado repetitivo, es fácil que alguien descifre la clave secreta WEP. Esto se conoce como ataque IV.
Los dispositivos móviles utilizan señales RF o tecnologías móviles para la comunicación. Si el dispositivo utiliza WAP, existen muchos niveles de seguridad: la autenticación anónima (cualquiera puede conectarse), la autenticación

del servidor (el terminal puede autenticarse frente al servidor) y la autenticación de doble vía (el cliente y el servidor deben autentificarse entre sí).
<Nivel 1>Ideas clave para el examen
<Cuerpo texto>A continuación, incluimos las ideas clave que debe recordar para el examen Security+:
<Sep-med>* **Protocolos y componentes de un sistema inalámbricos:** La base de la mayoría de los sistemas inalámbricos es WAP. Este utiliza WEP para proporcionar seguridad en un entorno inalámbrico. WTLS es la capa de seguridad de WAP. Este funciona de forma similar a TCP/IP.
* **Hardware utilizado en una red inalámbrica:** El punto de acceso (PA) inalámbrico forma parte de la red de cableado y, con posterioridad, actúa como el enrutador de los clientes inalámbricos. La mayoría del tiempo, un punto de acceso inalámbrico funcionan con más de un estándar 802.11. Los clientes inalámbricos se conectan a los puntos de acceso utilizando una tarjeta NIC inalámbrica.
* **Capacidades y limitaciones de los estándares de red 802.11x:** Los estándares actuales para los protocolos inalámbricos son 802.11, 802.11a, 802.11b y 802.11g. El estándar 802.11n está bajo revisión y todavía no es un estándar formal.
* **Vulnerabilidades de las redes inalámbricas:** El principal método para obtener información sobre una red inalámbrica es el sondeo del sitio. Este puede llevarse a cabo con un ordenador y una tarjeta 802.11. Las redes inalámbricas están sujetas a los mismos ataques que la redes de cableado.
* **Protocolos de seguridad inalámbrica:** Es estándar 802.11i se suele conocer como WPA2. Es una mejora de estándares anteriores como WEP (*Wired Equivalent Privacy*, Privacidad equivalente a cableado) y WPA (*Wi-Fi Protected Access*, Acceso Protegido Wi-Fi), que son mucho más débiles.
<Nivel 1>Prueba de evaluación
<Sep-med>1. ¿Qué protocolo se utiliza principalmente para habilitar el acceso a Internet desde un teléfono móvil o una PDA?
A. WEP. **B.** WTLS. **C.** WAP. **D.** WOP.
2. ¿Qué protocolo funciona en 2.4GHz y tiene un ancho de banda de 1 o 2 Mbps?
A. 802.11. **B.** 802.11a. **C.** 802.11b. **D.** 802.11g.
3. Está diseñando un plan para implementar una red inalámbrica para la alta administración. De repente, un vicepresidente paranoico plantea cuestiones de seguridad. ¿Qué protocolo se utiliza para proporcionar seguridad en una red inalámbrica y se considera equivalente del de una red de cableado?
A. WAP. **B.** WTLS. **C.** WPA2. **D.** IR.
4. ¿Cuál de las siguientes opciones es una de las vulnerabilidades principales en un entorno inalámbrico?
A. Decodificación de software. **B.** Husmeo de IP. **C.** Hueco en WAP. **D.** Sondeo de sitio.
5. ¿Cuál de las siguientes opciones es sinónimo de filtrado MAC?
A. TKIP. **B.** Bloqueo de red. **C.** EAP-TTLS. **D.** MAC seguro.
6. ¿Cuál de los siguientes estándares de 802.11 se suele conocer como WPA2?
A. 802.11a. **B.** 802.11b. **C.** 802.11i. **D.** 802.11n.
7. ¿Cuál de los siguientes estándares de 802.11 proporciona ancho de banda de hasta 300 Mbps?
A. 802.11n. **B.** 802.11i. **C.** 802.11g. **D.** 802.11b.
8. ¿Con cuál de los siguientes protocolos inalámbricos se suele asociar un ataque IV?
A. WEP. **B.** WAP. **C.** WPA. **D.** WPA2.
9. ¿Qué tipo de cifrado utiliza CCMP?
A. EAP. **B.** DES. **C.** AES. **D.** IV.
10. ¿Qué tecnología de cifrado se asocia con WPA?
A. TKIP. **B.** CCMP. **C.** WEP. **D.** LDAP.
11. ¿Cuál de las siguientes opciones no es una de las tres tecnologías de transmisión utilizadas para comunicarse en el estándar 802.11?
A. DSSS. **B.** FHSS. **C.** VITA. **D.** OFDM.
12. ¿Cuál es el tamaño del vector de inicialización (IV) que utiliza WEP para el cifrado?
A. 6-bit. **B.** 24-bit. **C.** 56-bit. **D.** 128-bit.
13. ¿Cuál de las siguientes opciones es un leguaje de secuencias de comando con WAP habilitado al que los dispositivos pueden responder?
A. WXML. **B.** Winsock. **C.** WIScript. **D.** WMLScript.
14. ¿Cuál de los siguientes niveles de autenticación con WAP requiere que los dos extremos de la conexión se autentique para confirmar la validez?
A. Relajado. **B.** De doble vía. **C.** Servidor. **D.** Anónimo.
15. ¿Cuál de las siguientes opciones gestiona la información de la sesión y la conexión entre los dispositivos inalámbricos?
A. WSP. **B.** WPD. **C.** WPT. **D.** WMD.
16. ¿Cuál de las siguientes opciones proporciona servicios similares a TCP y UDP para WAP?
A. WTLS. **B.** WDP. **C.** WTP. **D.** WFMD.
17. ¿Cuál de los siguientes niveles de autenticación con WAP permite que casi todo el mundo se conecte al portal inalámbrico?
A. Relajado. **B.** De doble vía. **C.** Servidor. **D.** Anónimo.
18. Si la interconexión entre el servidor WAP e Internet no está cifrado, pueden interceptarse los paquetes entre los dispositivos. ¿Cómo se llama esta vulnerabilidad?
A. Husmear paquetes. **B.** Rellenar el hueco. **C.** Hombre en el medio. **D.** Promesa rota.
19. WAP utiliza una versión más pequeña de HTML para Internet. Este se conoce como:

A. DSL. **B.** HSL. **C.** WML. **D.** OFML.
20. ¿Cuál es el tamaño del contenedor de TKIP que se coloca alrededor del cifrado WEP con una clave basada en elementos como la dirección MAC de su máquina y el número de serie del paquete?
A. 128-bit. **B.** 64-bit. **C.** 56-bit. **D.** 12-bit.
<Nivel 1>Respuestas de la prueba de evaluación
<Sep-med>1. C. WAP es un estándar internacional abierto para aplicaciones que utilizan conexiones inalámbricas.
2. A. 802.11 funciona en 2.4GHz y tiene un ancho de banda de 1 o 2 Mbps.
3. C. WPA2 se diseñó para proporcionar seguridad en una red inalámbrica y se considera equivalente del de una red de cableado e implementa elementos del estándar 802.11i.
4. D. Un sondeo de sitio es el proceso de monitorizar una red inalámbrica utilizando un ordenador, un controlador inalámbrico y un software de análisis. Este es fácil de conseguir y difícil de detectar.
5. B. El término bloqueo de red es sinónimo de filtrado MAC.
6. C. El estándar 802.11i se suele conocer como WPA2.
7. A. El estándar 802.11n proporciona ancho de banda de hasta 300 Mbps.
8. A. Un ataque IV se suele asociar con el protocolo inalámbrico WEP.
9. C. CCMP utiliza un cifrado AES de 128-bit.
10. A. La tecnología de cifrado asociada con WPA es TKIP.
11. C. Se utilizan tres tecnologías para comunicarse en el estándar 802.11 y proporcionan compatibilidad retroactiva con 802.11b DSSS, FHSS y OFDM. VITA (*Volunteer Income Tax Assistance*, Asistencia de impuestos de entrada voluntaria) no es una tecnología de transmisión.
12. B. El tamaño del vector de inicialización (IV) que utiliza WEP para el cifrado es 24-bit.
13. D. Los dispositivos con WAP habilitado responden a secuencias de comando utilizan un entorno WMLScript.
14. B. La autenticación de doble vía requiere que los dos extremos de la conexión se autentiquen para confirmar la validez.
15. A. WSP gestiona la información de la sesión y la conexión entre los dispositivos inalámbricos.
16. C. WTP proporciona servicios similares a TCP y UDP para WAP.
17. D. La autenticación anónima permite que casi todo el mundo se conecte al portal inalámbrico.
18. A. Si la interconexión entre el servidor WAP e Internet no está cifrado, pueden interceptarse los paquetes entre los dispositivos y se conoce como husmear paquetes.
19. C. WAP utiliza una versión más pequeña de HTML para Internet. Este se conoce como WML.
20. A. El tamaño del contenedor de TKIP que se coloca alrededor del cifrado WEP con una clave basada en elementos como la dirección MAC de su máquina y el número de serie del paquete es de 128-bit.

Anexo II: Texto original

Chapter 2: Infrastructure and Connectivity

Infrastructure and Connectivity

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **1.1 Explain the security function and purpose of network devices and technologies.**
  - Firewalls
  - Routers
  - Switches
  - Load Balancers
  - Proxies
  - Web security gateways
  - VPN concentrators
  - Spam filter, all-in-one security appliances
  - Web application firewall vs. network firewall
- ✓ **1.3 Distinguish and differentiate network design elements and compounds.**
  - DMZ
  - Subnetting
  - VLAN
  - NAT
  - Remote Access
  - Telephony
  - Virtualization

- ✓ **1.4 Implement and use common protocols.**
  - IPSec
  - SNMP
  - SSH
  - DNS
  - TLS
  - SSL
  - TCP/IP
  - FTPS
  - HTTPS
  - SFTP
  - SCP
  - ICMP
  - IPv4 vs. IPv6
- ✓ **1.5 Identify commonly used default network ports.**
  - FTP
  - SFTP
  - FTPS
  - TFTP
  - TELNET
  - HTTP
  - HTTPS
  - SCP
  - SSH
  - NetBIOS
- ✓ **2.8 Exemplify the concepts of confidentiality, integrity, and availability (CIA).**
- ✓ **4.2 Carry out appropriate procedures to establish host security.**
  - Virtualization

This chapter introduces the hardware used within the network. Your network is composed of a variety of *media* and devices that both facilitate communications and provide security. Most of these devices (such as routers, modems, and PBX systems) provide external connectivity from your network to other systems and networks. To provide reasonable security, you must know how these devices work and how they provide, or fail to provide, security.

This chapter deals with issues of infrastructure, network ports, and common protocols. They're key components of the Security+ exam, and it's necessary that you understand them to secure your network. Like many certification exams, though, the Security+ test requires you to know not only current technologies but some legacy components as well.

Mastering TCP/IP

TCP/IP has been a salvation for organizations that need to connect different systems together to function as a unified whole. Unfortunately, a downside that comes with an easy-to-use, well-documented network that has been around for many years is numerous holes. You can easily close most of these holes in your network, but you must first know about them.

You need to have a good understanding of the processes TCP/IP uses in order to know how attacks on TCP/IP work. The emphasis in this section is on the types of connections and services. If you're weak in those areas, you'll do well to supplement your study with basic networking information that can be found on the Web.

The following sections delve into issues related to TCP/IP and security. Many of these issues will be familiar to you if you've taken the Network+ or Server+ exam from CompTIA. If there are any gaps in your knowledge of the topics, however, be sure to read these sections carefully.

When discussing networking, most refer to the seven-layer OSI model—long considered the foundation for how networking protocols should operate. TCP/IP precedes the creation of the OSI model, and that is why it carries out the same operations but does so with four layers instead of seven.

Working with the TCP/IP Suite

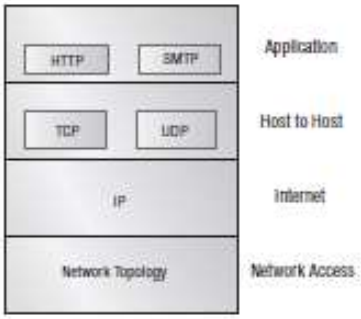
The TCP/IP suite is broken into four architectural layers:

- Application layer
- Host-to-Host or Transport layer
- Internet layer
- Network Access layer (also known as the Network Interface layer or the Link layer)

Computers using TCP/IP use the existing physical connection between the systems. TCP/IP doesn't concern itself with the network topology, or physical connections. The network controller that resides in a computer or host deals with the physical protocol, or topology. TCP/IP communicates with that controller and lets the controller worry about the network topology and physical connection.

In TCP/IP parlance, a computer on the network is a *host*. A host is any device connected to the network that runs a TCP/IP protocol suite, or stack. Figure 2.1 shows the four layers in a TCP/IP protocol stack. Notice that this drawing includes the physical, or network, topology. Although it isn't part of TCP/IP, the topology is essential to conveying information on a network..

FIGURE 2.1 The TCP/IP architecture layers



The four layers of TCP/IP have unique functions and methods for accomplishing work. Each layer talks to the layers that reside above and below it. Each layer also has its own rules and capabilities.

The following sections discuss the specific layers of TCP/IP as well as the common protocols used in the stack and how information is conveyed between the layers. I also discuss some of the more common methods used to attack TCP/IP-based networks.

Encapsulation, the process used to pass messages between the layers in TCP/IP, is briefly discussed in the next section after the layers have been covered.

The Application Layer

The *Application layer* is the highest layer of the suite. It allows applications to access services or protocols to exchange data. Most programs, such as web browsers, interface with TCP/IP at this level. The most commonly used Application layer protocols are as follows:

Hypertext Transfer Protocol *Hypertext Transfer Protocol (HTTP)* is the protocol used for web pages and the World Wide Web. HTTP applications use a standard language called *Hypertext Markup Language (HTML)*. HTML files are normal text files that contain special coding that allows graphics, special fonts, and characters to be displayed by a web browser or other web-enabled applications.

HTTP Secure *HTTP Secure (HTTPS)* is the protocol used for "secure" web pages that a user should see when they must enter personal information such as credit card numbers, passwords, and other identifiers. It combines HTTP with SSL/TLS to provide encrypted communication. The default port is 443 and the URL begins with `https://` instead of `http://`. The protocol was originally created by Netscape for use with their browser and became a finalized standard with RFC 2818 (which can be found at: `http://www.ietf.org/rfc/rfc2818.txt`).

File Transfer Protocol *File Transfer Protocol (FTP)* is an application that allows connections to FTP servers for file uploads and downloads. FTP is a common application used to transfer files between hosts on the Internet but is inherently insecure. A number of options have been released to try to create a more secure protocol including *FTP over SSL (FTPS)*, which adds support for SSL cryptography, and *SSH File Transfer Protocol (SFTP)*, which is also known as Secure FTP.

An alternative utility for copying files is *Secure Copy (SCP)*, which combines an old remote copy program (RCP) from the first days of TCP/IP with SSH. On the opposite end of the spectrum, from a security standpoint, is the *Trivial File Transfer Protocol (TFTP)*, which can be configured to transfer files between hosts without any user interaction (unattended mode) and should be avoided at all costs.

Simple Mail Transfer Protocol *Simple Mail Transfer Protocol (SMTP)* is the standard protocol for email communications. SMTP allows email clients and servers to communicate with each other for message delivery.

Telnet *Telnet* is an interactive terminal emulation protocol. It allows a remote user to conduct an interactive session with a Telnet server. This session can appear to the client as if it were a local session.

Domain Name System *Domain Name System (DNS)* allows hosts to resolve hostnames to an Internet Protocol (IP) address. IP is discussed in the section on the Internet layer.

Routing Information Protocol *Routing Information Protocol (RIP)* allows routing information to be exchanged between routers on an IP network.

Simple Network Management Protocol *Simple Network Management Protocol (SNMP)* is a management tool that allows communications between network devices and a management console. Most routers, bridges, and intelligent hubs can communicate using SNMP.

Post Office Protocol *Post Office Protocol (POP)* is a protocol used in many email systems. It allows for advanced features and is a standard interface in many email servers. POP is used for receiving email.

One of the key things to know when securing any network is that you are running only the protocols needed for operations. Make certain that *antiquated protocols*—those once needed but now no longer used—are removed. If you do not remove them, you are leaving an opening for an attacker to access your system through weaknesses in that protocol.

The Host-to-Host or Transport Layer

The *Host-to-Host layer*, also called the *Transport layer*, provides the Application layer with session and datagram communications services. The *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)* operate at this layer. These two protocols provide a huge part of the functionality of the TCP/IP network:

TCP TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets. Two hosts communicate packet results to each other. TCP also makes sure that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.

UDP UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP. The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for acknowledging the correct reception of the data.

The Internet Layer

The *Internet layer* is responsible for routing, IP addressing, and packaging. The Internet layer protocols accomplish most of the behind-the-scenes work in establishing the ability to exchange information between hosts. Here are the four standard protocols of the Internet layer:

Internet Protocol *Internet Protocol (IP)* is a routable protocol that is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it doesn't verify it for accuracy. Accuracy checking is the responsibility of TCP. IP determines if a destination is known and, if so, routes the information to that destination. If the destination is unknown, IP sends the packet to the router, which sends it on.

Address Resolution Protocol *Address Resolution Protocol (ARP)* is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a *Media Access Control (MAC)* address. MAC addresses are used to identify hardware network devices such as a network interface card (NIC).

You'll notice the acronym *MAC* used a lot. It's also used to identify *Mandatory Access Control*, which defines how access control operates in an authentication model. You'll also see *MAC* used in cryptography, where it stands for *Message Authentication Code*. This MAC verifies that an algorithm is accurate.

Internet Control Message Protocol *Internet Control Message Protocol (ICMP)* provides maintenance and reporting functions. It's used by the Ping program. When a user wants to test connectivity to another host, they can enter the PING command with the IP address, and the user's system will test connectivity to the other host's system. If connectivity is good, ICMP will return data to the originating host. ICMP will also report if a destination is unreachable. Routers and other network devices report path information between hosts with ICMP.

Internet Group Management Protocol *Internet Group Management Protocol (IGMP)* is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts. This is different from a broadcast, which all users in a network receive.

The Network Access Layer

The lowest level of the TCP/IP suite is the *Network Access (or Interface) layer*. This layer is responsible for placing and removing packets on the physical network through communications with the network adapters in the host. This process allows TCP/IP to work with virtually any type of network topology or technology with little modification. If a new physical network topology were installed—say, a 10GB Fiber Ethernet connection—TCP/IP would only need to know how to communicate with the network controller in order to function properly. TCP/IP can also communicate with more than one network topology simultaneously. This allows the protocol to be used in virtually any environment.

IPv4 vs. IPv6

The TCP/IP protocol suite in use today has been around since the earliest days of the Internet—prior to it even being known by that name. The remarkable fact that it has been able to scale to the level it is used at today is testament to the forward thinking of those involved in its creation.

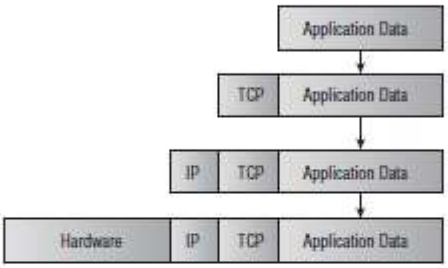
Several years back, however, a panic arose amid fears that there would not be enough IP addresses to assign to every host needing to connect. The current numbering system, known as IP version 4 (IPv4) even though there really weren't publically released prior versions, is what is described throughout this chapter and still widely used today. IP version 6 (IPv6) was introduced several years ago to replace IPv4 but has failed to do so, and most systems currently support both at the Internet layer.

Key things to know for the exam are that IPv6 supports 128-bit addresses, while IPv4 supports 32-bit addresses (see "Network Address Translation" later in this chapter), and IPv6 includes mandatory IPSec security (see "Internet Protocol Security" later in this chapter).

Understanding Encapsulation

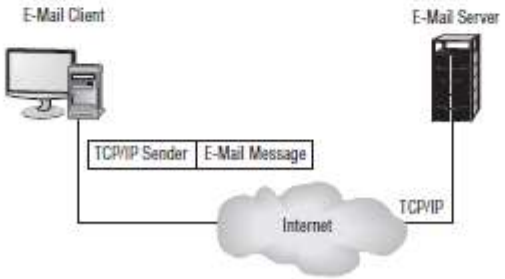
One of the key points in understanding this layering process is the concept of *encapsulation*. Encapsulation allows a transport protocol to be sent across the network and utilized by the equivalent service or protocol at the receiving host. Figure 2.2 shows how email is encapsulated as it moves from the application protocols through the transport and Internet protocols. Each layer adds header information as the email moves down the layers.

FIGURE 2.2 The encapsulation process of an email message



Transmission of the packet between the two hosts occurs through the physical connection in the network adapter. Figure 2.3 illustrates this process between two hosts. What's shown in the figure isn't comprehensive but illustrates the process of message transmission.

FIGURE 2.3 An email message that an email client sent to an email server across the Internet



After it is encapsulated, the message is sent to the server. Notice that in Figure 2.3 the message is sent via the Internet; it could have just as easily been sent locally. The email client doesn't know how the message is delivered, and the server application doesn't care how the

message got there. This makes designing and implementing services such as email possible in a global or Internet environment.

Working with Protocols and Services

It's imperative that you have a basic understanding of protocols and services to pass this exam. Although it isn't a requirement, CompTIA recommends that you already hold the Network+ certification before undertaking this exam. In case you're weak in some areas, the following sections will discuss in more detail how TCP/IP hosts communicate with each other. I'll discuss the concepts of ports, handshakes, and application interfaces. The objective isn't to make you an expert on this subject but to help you understand what you're dealing with when attempting to secure a TCP/IP network.

The majority of the discussion in this book focuses on TCP/IP as the networking protocol since it is used in almost every implementation. Know, however, that TCP/IP is not the only networking protocol and Microsoft's implementation of *NetBIOS* (Network Basic Input Output System) was a default in early versions of Windows. Since then, NetBIOS has been adapted to run on top of TCP/IP and is still widely used for name resolution and registration in Windows-based environments.

Well-Known Ports

Simply stated, *ports* identify how a communication process occurs. Ports are special addresses that allow communication between hosts. A port number is added from the originator, indicating which port to communicate with on a server. If a server has a port defined and available for use, it will send back a message accepting the request. If the port isn't valid, the server will refuse the connection. The *Internet Assigned Numbers Authority (IANA)* has defined a list of ports called *well-known ports*.

You can see the full description of the ports defined by IANA on the following website: `www.iana.org/assignments/port-numbers`. Many thousands of ports are available for use by servers and clients.

A port is nothing more than a bit of additional information added to either the TCP or UDP message. This information is added in the header of the packet. The layer below it encapsulates the message with its header.

Many of the services you'll use in the normal course of utilizing the Internet use the TCP port numbers identified in Table 2.1. Table 2.2 identifies some of the more common, well-known UDP ports. You will note that some services utilize both TCP and UDP ports, while many use only one or the other.

TABLE 2.1 Well-known TCP ports

TCP Port Number	Service
20	FTP (data channel)
21	FTP (control channel)
22	SSH and SCP
23	Telnet
25	SMTP
49	TACACS authentication service
80	HTTP (used for the World Wide Web)
110	POP3
115	SFTP
119	NNTP
137	NetBIOS name service
138	NetBIOS datagram service
139	NetBIOS session service
143	IMAP
389	LDAP
443	HTTPS (used for secure web connections)
989	FTPS (data channel)
990	FTPS (control channel)

TABLE 2.2 Well-known UDP ports

UDP Port Number	Service
22	SSH and SCP
49	TACACS authentication service

UDP Port Number	Service
53	DNS name queries
69	Trivial File Transfer Protocol (TFTP)
80	HTTP (used for the World Wide Web)
137	NetBIOS name service
138	NetBIOS datagram service
139	NetBIOS session service
143	IMAP
161	SNMP
389	LDAP
989	FTPS (data channel)
990	FTPS (control channel)

The early documentation for these ports specified that ports below 1024 were restricted to administrative uses. However, enforcement of this restriction has been voluntary and is creating problems for computer security professionals. As you can see, each of these ports potentially requires different security considerations, depending on the application it's assigned for. All the ports allow access to your network; even if you establish a firewall, you must have these ports open if you want to provide email or web services.

In Exercise 2.1, I'll show you how to view the active TCP and UPD ports.

EXERCISE 2.1

View the Active TCP and UDP Ports

As an administrator, you should know what ports are active on your server. To view the active TCP and UDP ports, follow these steps:

1. Go to a command prompt. To do this in Windows, enter CMD at the Run prompt. On a Linux server, open a command window.

EXERCISE 2.1 *(continued)*

2. Enter the command **netstat**.

3. Few items should appear. Now enter the command **netstat -a**. The **-a** parameter tells the **netstat** command to display all the information.
4. Note the ports that are listed.

EXERCISE 2.1 *(continued)*

5. View the services file (*systemroot*\system32\drivers\etc\services in Windows or /etc/services in Linux). Although the file is not actively read by the system, this file lists the services and the ports used for the most common network operations.

TCP Three-Way Handshake

TCP, which is a *connection-oriented protocol*, establishes a session using a *three-way handshake*. A host called a *client* originates this connection. The client sends a TCP segment, or message, to the server. This client segment includes an *Initial Sequence Number (ISN)* for the connection and a window size. The server responds with a TCP segment that contains its ISN and a value indicating its buffer, or window size. The client then sends back an acknowledgment of the server's sequence number.

Figure 2.4 shows this three-way handshake occurring between a client and a server. When the session or connection is over, a similar process occurs, using four steps, to close the connection.

FIGURE 2.4 The TCP connection process

A web request uses the TCP connection process to establish the connection between the client and the server. After this occurs, the two systems communicate with each other; the server uses TCP port 80. The same thing occurs when an email connection is made, with the difference being that the client (assuming it's using POP3) uses port 110.

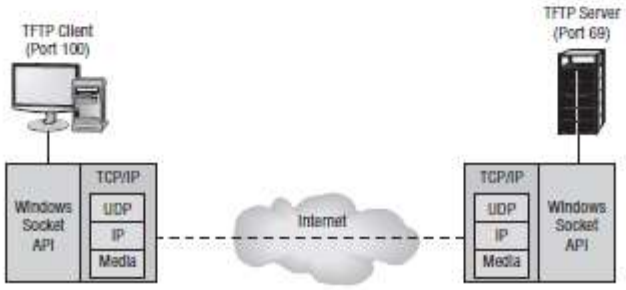
In this way, a server can handle many requests simultaneously. Each session has a different sequence number even though all sessions use the same port. All the communications in any given session use this sequence number to keep from confusing the sessions.

Application Programming Interface

Interfacing to TCP/IP is much simpler than interfacing to earlier network models. A well-defined and well-established set of *Application Programming Interfaces (APIs)* is available from most software companies. APIs allow programmers to create interfaces to the protocol. When a programmer needs to create a web-enabled application, they can call or use one of these APIs to make the connection, send or receive data, and end the connection. The APIs are prewritten, and they make the job considerably easier than manually coding all of the connection information.

Microsoft uses the *Windows Sockets (Winsock)* API to interface to the protocol. It can access either TCP or UDP protocols to accomplish the needed task. Figure 2.5 illustrates how Winsock connects to the TCP/IP protocol suite.

FIGURE 2.5 The Winsock interface



Distinguishing between Security Topologies

The *security topology* of your network defines the network design and implementation from a security perspective. Unlike a network topology, here we're concerned with access methods, security, and technologies used. Security topology covers four primary areas of concern:

- Design goals
- Security zones
- Technologies
- Business requirements

Setting Design Goals

When setting design goals for a security topology, you must deal with issues of confidentiality, integrity, availability, and accountability, all four of which are discussed continually throughout this book as they apply to various topics. Addressing these four issues as an initial part of your network design will help you ensure tighter security. You'll often see confidentiality, integrity, and availability referred to as the *CIA* of network security, but the accountability component is equally important—design goals must identify who is responsible for the various aspects of computer security. The next few sections introduce these four security components.

Confidentiality

Meeting the goal of *confidentiality* is to prevent or minimize unauthorized access to and disclosure of data and information. In many instances, laws and regulations require specific information confidentiality. For example, Social Security records, payroll and employee records, medical records, and corporate information are high-value assets. This information could create liability issues or embarrassment if it fell into the wrong hands. Over the last few years, there have been a number of cases in which bank account and credit card numbers were published on the Internet. The costs of these types of breaches of confidentiality far exceed the actual losses from the misuse of this information.

Confidentiality entails ensuring that data expected to remain private is seen only by those who should see it. Confidentiality is implemented through authentication and access controls.

If you address confidentiality issues early in the design phase, the steps that must be taken to minimize this exposure will become clear.

Integrity

Meeting the goal of *integrity* involves making sure that the data being worked with is the correct data. Information integrity is critical to a secure topology. Organizations work with and make decisions using the data they have available. If this information isn't accurate or is tampered with by an unauthorized person, the consequences can be devastating.

Take the case of a school district that lost all the payroll and employment records for the employees in the district. When the problem was discovered, the school district had no choice but to send out applications and forms to all the employees, asking them how long they had worked in the school district and how much they were paid. Integrity was jeopardized because the data was vulnerable and then lost.

You can think of integrity as the level of confidence you have that the data is what it's supposed to be—untampered with and unchanged. *Authentic, complete,* and *trustworthy* are often used to describe integrity in terms of data.

Availability

To meet the goal of *availability*, you must protect data and prevent its loss. Data that can't be accessed is of little value. If a mishap or attack brings down a key server or database, that information won't be available to the people who need it. This can cause havoc in an organization. Your job is to provide maximum availability to your users while ensuring integrity and confidentiality. The hardest part of this process is determining the balance you must maintain between these three aspects to provide acceptable security for the organization's information and resources.

The key to availability is that the data must be available when it's needed and accessible by those who need it.

Accountability

The final and often overlooked goal of design concerns *accountability*. Many of the resources used by an organization are shared among departments and individuals. If an error or incident occurs, who is responsible for fixing it? Who determines whether information is correct?

It's a good idea to be clear about who owns the data or is responsible for making sure that it's accurate. You should also be able to track and monitor data changes to detect and repair the data in the event of loss or damage. Most systems will track and store logs on system activities and data manipulation, and they will also provide reports on problems.

Real World Scenario

Compute Availability

Availability is often expressed in terms of *uptime*. High availability strives for 99.9999% uptime over the course of the year (24 hours a day, 7 days a week, 365 days a year). For this exercise, compute how long data wouldn't be available over the course of the year with the following availability percentages. For example, with 98% uptime, there is a 2% downtime of 525,600 minutes in a year. That means the data would be down for 10,512 minutes, or 71/3 days! Try your math on the following:

1. 99%
2. 99.9%
3. 99.99%
4. 99.999%
5. 99.9999%

The increments may seem small, but over the course of a year, they represent a significant difference in the amount of time data is and isn't available. Answers: (1.) 5,256 minutes, which is more than 87 hours or 3.5 days; (2.) 525 minutes, or a little less than 9 hours; (3.) 52.56 minutes; (4.) 5.25 minutes; (5.) about half a minute.

Creating Security Zones

Over time, networks can become complex beasts. What may have started as a handful of computers sharing resources can quickly grow to something resembling an electrician's nightmare. The networks may even appear to have lives of their own. It's common for a network to have connections among departments, companies, countries, and public access using private communication paths and through the Internet.

Not everyone in a network needs access to all the assets in the network. The term *security zone* describes design methods that isolate systems from other systems or networks. You can isolate networks from each other using hardware and software. A router is a good example of a hardware solution: You can configure some machines on the network to be in a certain address range and others to be in a different address range. This separation makes the two networks invisible to each other unless a router connects them. Some of the newer data switches also allow you to partition networks into smaller networks or private zones.

When discussing security zones in a network, it's helpful to think of them as rooms. You may have some rooms in your house or office that anyone can enter. For other rooms, access is limited to specific individuals for specific purposes. Establishing security zones is

a similar process in a network: Security zones allow you to isolate systems from unauthorized users. Here are the four most common security zones you'll encounter:

- Internet
- Intranet
- Extranet
- Demilitarized zone (DMZ)

Real World Scenario

Accountability Is More than a Catchphrase

Accountability, like common sense, applies to every aspect of information technology. Several years ago, a company that relied on data that could never be re-created wrote shell scripts to do backups early in the morning when the hosts were less busy. Operators at those machines were told to insert a tape in the drive around midnight and check back at 3:00 a.m. to make certain that a piece of paper had been printed on the printer, signaling the end of the job. If the paper was there, they were to remove the tapes and put them in storage; if the paper was not there, they were to call for support.

The inevitable hard drive crash occurred on one of the hosts one morning, and an IT "specialist" was dispatched to swap it out. The technician changed the hard drive and then asked for the most recent backup tape. To his dismay, the data on the tape was two years old. The machine crash occurred before the backup operation ran, he reasoned, but the odds of rotating exactly two years' worth of tapes was highly unlikely. Undaunted, he asked for the tape from the day before, and found that the data on it was also two years old.

Beginning to sweat, he found the late shift operator for that host and asked her if she was making backups. She assured him that she was and that she was rotating the tapes and putting them away as soon as the paper printed out. Questioning her further on how the data could be so old, she said she could verify her story because she also kept the pieces of paper that appeared on the printer each day. She brought out the stack and handed them to him. They all reported the same thing—*tape in drive is write protected*.

Where did the accountability lie in this true story? The operator was faithfully following the procedures given to her and going through the procedures to back up the company's information each night. She thought the fact that the tape was protected represented a good thing. It turned out that all the hosts had been printing the same message, but the operator lacked the information she needed to realize there was a problem, leading to the company not having any backups for two years.

The problem lay not with the operator but with the training she was given. Had she been shown what correct and incorrect backup completion reports looked like, the data would never have been lost.

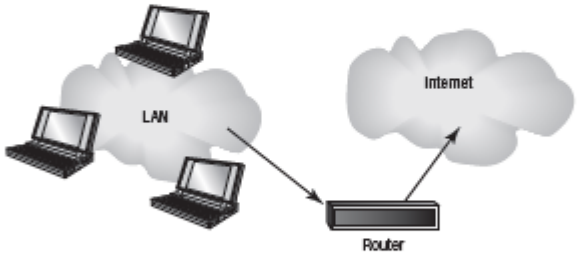
The next few sections identify the topologies used to create security zones to provide security, as well as designing them. The Internet has become a boon to individuals and to businesses, but it creates a challenge for security. By implementing intranets, extranets, and DMZs, you can create a reasonably secure environment for your organization.

The Internet

The *Internet* is a global network that connects computers and individual networks together. It can be used by anybody who has access to an Internet portal or an Internet service provider (ISP). In this environment, you should have a low level of trust in the people who use the Internet. You must always assume that the people visiting your website may have bad intentions; they may want to buy your product or hire your firm, or they may want to bring your servers to a screaming halt. Externally, you have no way of knowing until you monitor their actions. Because the Internet involves such a high level of anonymity, you must always safeguard your data with the utmost precautions.

Figure 2.6 illustrates an Internet network and its connections.

FIGURE 2.6 A typical LAN connection to the Internet



Sometimes the data leaving a network can be as much a sign of trouble as the data entering it. Examining data leaving the network for signs of malicious traffic is a fairly new field of computer security and is known as *extrusion*.

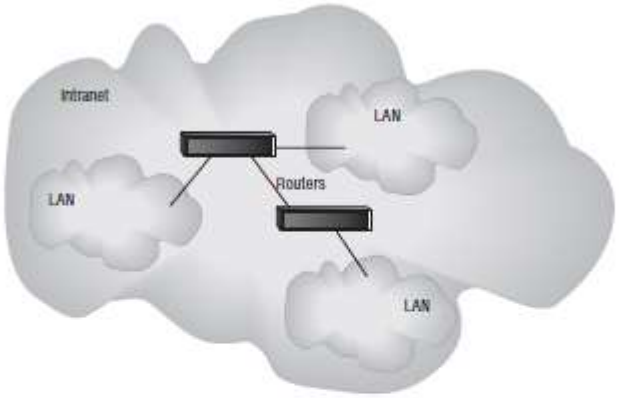
Intranets

Intranets are private networks implemented and maintained by an individual company or organization. You can think of an intranet as an Internet that doesn't leave your company; it's internal to the company, and access is limited to systems within the intranet. Intranets use the same technologies used by the Internet. They can be connected to the Internet but can't be accessed by users who aren't authorized to be part of them; the anonymous user of

the Internet is instead an authorized user of the intranet. Access to the intranet is granted to trusted users inside the corporate network or to users in remote locations.

Figure 2.7 displays an intranet network.

FIGURE 2.7 An intranet network

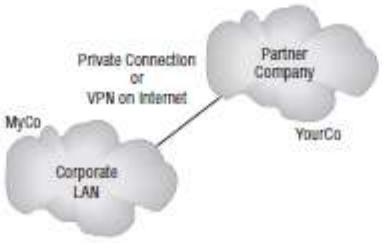


Extranets

Extranets extend intranets to include outside connections to partners. The partners can be vendors, suppliers, or similar parties who need access to your data for legitimate reasons. An extranet allows you to connect to a partner via a private network or a connection using a secure communications channel across the Internet. Extranet connections involve connections between trustworthy organizations.

An extranet is illustrated in Figure 2.8. Note that this network provides a connection between the two organizations. The connection may be through the Internet; if so, these networks would use a tunneling protocol to accomplish a secure connection.

FIGURE 2.8 A typical extranet between two organizations

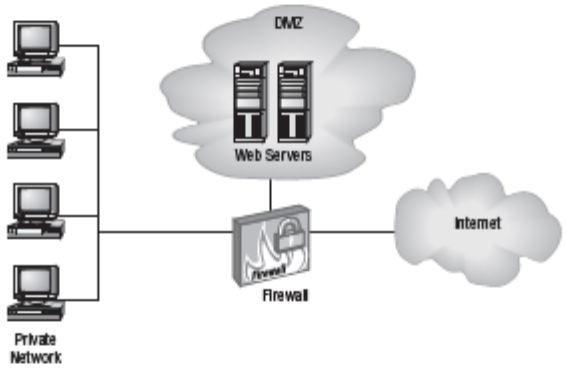


Demilitarized Zone

A *demilitarized zone (DMZ)* is an area where you can place a public server for access by people you might not trust otherwise. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources. This can be accomplished using firewalls to isolate your network.

When establishing a DMZ, you assume that the person accessing the resource isn't necessarily someone you would trust with other information. Figure 2.9 shows a server placed in a DMZ. Notice that the rest of the network isn't visible to external users. This lowers the threat of intrusion in the internal network.

FIGURE 2.9 A typical DMZ



Anytime you want to separate public information from private information, a DMZ is an acceptable option.

The easiest way to create a DMZ is to use a firewall that can transmit in three directions:

- to the internal network
- to the external world (Internet)
- to the public information you're sharing (the DMZ)

From there, you can decide what traffic goes where; for example, HTTP traffic would be sent to the DMZ, and email would go to the internal network.

A host that exists outside the DMZ and is open to the public is often called a *bastion host*. Routers and firewalls, because of where they must exist, often constitute bastion hosts.

Designing Security Zones

Security zone design is an important aspect of computer security. You can use many different approaches to accomplish a good solid design. Some of the design trade-offs involve risk and money. You can create layers of security to protect systems from less-secure connections, and you can use Network Address Translation (NAT) (discussed later) to hide resources. New methods and tools to design secure networks are being introduced on a regular basis. It's important to remember that after you have a good security design, you should revisit it on a regular basis based on what you learn about your security risks.

Working with Newer Technologies

One of the nice things about technology is that it's always changing. One of the bad things about technology is that it's always changing. Several relatively new technologies have become available to help you create a less-vulnerable system. The four technologies this section will focus on are:

- virtualization
- virtual local area networks (VLANs)
- Network Address Translation
- tunneling

These technologies allow you to improve security in your network at little additional cost.

Virtualization Technology

Virtualization is easily the technology du jour, with VMware, one of the largest vendors of such technology, counting 100 percent of the Fortune 100 as part of their customer base. In addition to proprietary solutions, there are open source solutions as well, with Xen and VirtualBox being the best-known examples.

Virtualization technology allows you to take any single physical device and hide its characteristics from users—in essence allowing you to run multiple items on one device and make them appear as if they are stand-alone entities. For example, workstations can run only one operating system at a time. Using virtualization, it is possible for a workstation running Windows 7 to also be running Fedora, Red Hat, Windows Server 2008, and any number of other operating systems within virtual windows. The developer working on code can move between windows, cutting and pasting if they choose, and do all they need to do on one machine without having to run four different workstations. Thanks to virtualization, the workstation can run multiple operating systems, multiple versions of the same operating system, multiple applications, and so on.

Just as a workstation can be virtualized, so too can a server. A single server can host multiple logical machines. By using one server to do the functions of many, you can immediately gain cost savings in terms of hardware, utility, infrastructure, and so on.

As wonderful as virtualization is, from a security standpoint it can present challenges. A user accessing the system could have access to everything on the system (not just within their logical machine) if they could override the physical layer protection. As of this writing, the

threat of that occurring has been far more rumored than performed, but with virtualization growing in popularity, it is a safe bet that virtual machines will become a popular target of miscreants in coming years.

Virtual Local Area Networks

A *virtual local area network (VLAN)* allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access. You can also set up VLANs to control the paths that data takes to get from one point to another. A VLAN is a good way to contain network traffic to a certain area in a network.

Think of a VLAN as a network of hosts that act as if they're connected by a physical wire even though there is no such wire between them.

On a LAN, hosts can communicate with each other through broadcasts, and no forwarding devices, such as routers, are needed. As the LAN grows, so too does the number of broadcasts. Shrinking the size of the LAN by segmenting it into smaller groups (VLANs) reduces the size of the broadcast domains. The advantages of doing this include reducing the scope of the broadcasts, improving performance and manageability, and decreasing dependence on the physical topology. From the standpoint of this exam, however, the key benefit is that VLANs can increase security by allowing users with similar data sensitivity levels to be segmented together.

Figure 2.10 illustrates the creation of three VLANs in a single network.

Network Address Translation

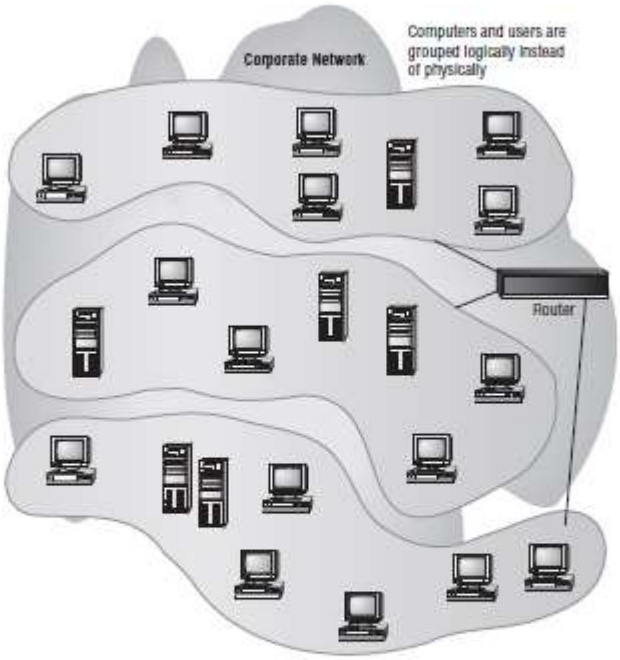
Network Address Translation (NAT) creates a unique opportunity to assist in the security of a network. Originally, NAT extended the number of usable Internet addresses. Now it allows an organization to present a single address to the Internet for all computer connections. The NAT server provides IP addresses to the hosts or systems in the network and tracks inbound and outbound traffic.

A company that uses NAT presents a single connection to the network. This connection may be through a router or a NAT server. The only information that an intruder will be able to get is that the connection has a single address.

NAT effectively hides your network from the world, making it much harder to determine what systems exist on the other side of the router. The NAT server effectively operates as a firewall for the network. Most new routers support NAT; it provides a simple, inexpensive firewall for small networks.

It's important to understand that NAT acts as a proxy between the local area network (which can be using private IP addresses) and the Internet. Not only can NAT save IP addresses, but it can also act as a firewall.

FIGURE 2.10 A typical segmented VLAN



Most NAT implementations assign internal hosts private IP address numbers and use public addresses only for the NAT to translate to and communicate with the outside world. The private address ranges, all of which addresses are non-routable, are as follows:

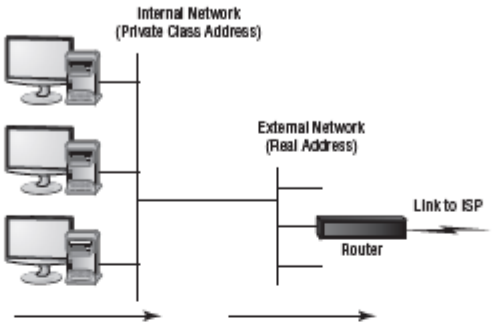
10.0.0.0–10.255.255.255

172.16.0.0–172.31.255.255

192.168.0.0–192.168.255.255

Figure 2.11 shows a router providing NAT services to a network. The router presents a single address for all external connections on the Internet.

FIGURE 2.11 A typical Internet connection to a local network



In addition to NAT, Port Address Translation (PAT) is possible. Whereas NAT can use multiple public IP addresses, PAT uses a single one and shares the port with the network. Because it is using only a single port, PAT is much more limited and typically used only on small and home-based networks. Microsoft's Internet Connection Sharing is an example of a PAT implementation.

IP addressing is a subject on the Network+ exam, as opposed to Security+, but CompTIA still expects you to know the basics. In addition to understanding the concept behind NAT, you should know that subnetting is how networks are divided. RFCs 1466 and 1918 detail subnetting and can be found at `http://www.faqs.org/rfcs/`.

Tunneling

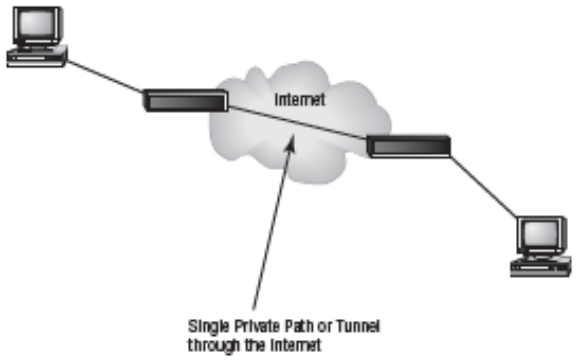
Tunneling refers to creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually agreed-upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network.

Tunneling protocols usually include data security as well as encryption. Several popular standards have emerged for tunneling, with the most popular being the Layer 2 Tunneling Protocol (L2TP).

Tunneling sends private data across a public network by placing (encapsulating) that data into other packets. Most tunnels are virtual private networks (VPNs).

Figure 2.12 shows a connection being made between two networks across the Internet. To each end of the network, this appears to be a single connection.

FIGURE 2.12 A typical tunnel



Telephony

When telephone technology is married with information technology, the result is known as *telephony*. A breach in your telephony infrastructure is just as devastating as any other violation and can lead to the loss of valuable data.

With the exodus from land lines to Voice over IP (VoIP) in order for companies to save money in full swing, it is imperative that you treat this part of the network the same as you would any other. VOIP can be easily sniffed with tools such as Cain & Abel (`http://www.oxid.it/`) and is susceptible to Denial of Service (DoS) attacks because it rides on UDP. There is also the outage issue with VoIP in cases where the data network goes down and you lose the telephony as well.

As an example of some of the information available, SecureLogix markets a voice firewall (`http://www.securelogix.com/ip-telephony-security.html`), and Cisco has published a white paper titled "IP Telephony Security in Depth" (`http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.pdf`).

From a security standpoint, the biggest problem with VoIP and data being on the same line is that they are then both vulnerable in the event of a PBX (private branch exchange) attack. For more information about PBX, see `http://www.pbxinfo.com/`.

Working with Business Requirements

The final component of security design is working with business requirements. A number of chapters in this book focus on the issue of understanding business requirements and working with policies and standards. For this discussion, simply know that there is no one-size-fits-all solution as straightforward as the other three areas (design goals, security zones, and technology) may seem, because every company will have different business requirements, including a different level of risk they are willing to accept and different regulations they must adhere to.

Understanding Infrastructure Security

As the name implies, an *infrastructure* is the basis for all the work occurring in your organization. *Infrastructure security* deals with the most basic aspect of how information flows and how work occurs in your network and systems. When discussing infrastructures, keep in mind that this includes servers, networks, network devices, workstations, and the processes in place to facilitate work.

To evaluate the security of your infrastructure, you must examine the hardware and its characteristics as well as the software and its characteristics. Each time you add a device, change configurations, or switch technologies, you're potentially altering the fundamental security capabilities of your network. Just as a chain is no stronger than its weakest link, it can also be said that a network is no more secure than its weakest node.

Networks are tied together using the Internet and other network technologies, thereby making them vulnerable to any number of attacks. The job of a security professional is to eliminate the obvious threats, to anticipate how the next creative assault on your infrastructure might occur, and to be prepared to neutralize it before it happens.

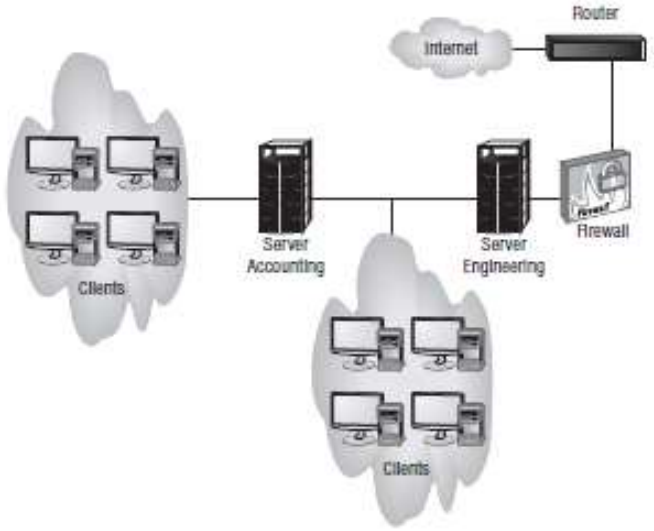
The following sections deal with the hardware and software components that make up a network.

Working with Hardware Components

Network hardware components include physical devices such as routers, servers, firewalls, workstations, and switches. Figure 2.13 depicts a typical network infrastructure and some of the common hardware components in the environment. From a security perspective, this infrastructure is much more than just the sum of all its parts. You must evaluate your network from the standpoint of each and every device within it. It cannot be overstated: The complexity of most networks makes securing them extremely complicated. To provide reasonable security, you must evaluate every device to determine its unique strengths and vulnerabilities.

Notice in this figure that the network we'll be evaluating has Internet connections. Internet connections expose your network to the highest number of external threats. These threats can come from virtually any location worldwide.

FIGURE 2.13 A typical network infrastructure



Real World Scenario

Updating Your Infrastructure List

As an administrator, you have to deal with a variety of devices every day. Not only must you attend to the needs of the servers, but you must also maintain Internet access, manage a plethora of users and workstations, and keep everything running smoothly. You can have firewall after firewall in place, but if you're allowing a salesperson to dial in from the road with minimal safeguards, that connection becomes the baseline of your security.

Keeping track of your organization's hardware is therefore a fairly important task, which is why you should survey your network and compile an infrastructure list. If you've already done this in the past, now is a great time to update that list. While doing this, make a note of all the devices that are connected—permanently or intermittently—to your network. Here are some questions you should try to answer:

1. How many servers are there? What is the function of each, and what level of security applies to each?

2. How many workstations are there? What operating systems are they running? How do they connect to the network (cabling, wireless, dial-in)?
3. How does data leave the network (routers, gateways)? How secure is each of those devices? Are firewalls or other devices impeding traffic?
4. What else is connected to the network (modems and so on) that can be used to access it?

In all honesty, this information should already exist and be readily accessible. If your organization is like most others, though, the information doesn't exist, and devices are added as needed with the intent of creating documentation at some future point in time. There is no better time than the present to create it.

One issue to watch out for is the "It can't happen to me/us!" attitude many seem to have. Be prepared to handle it by explaining that it can indeed happen and actively doing all you can to prevent it.

Working with Software Components

Hardware exists to run software. The software is intended to make the hardware components easy to configure and easy to support. To a certain extent, however, that software can also make the hardware easy to bypass.

The network infrastructure illustrated at the beginning of the chapter in Figure 2.1 includes servers, workstations running operating systems, a router, a firewall (and there may be some that run as applications on servers), and dedicated devices that have their own communications and control programs. This situation leaves networks open to attacks and security problems because many of these systems work independently.

Many larger organizations have built a single area for network monitoring and administrative control of systems. This centralization lets you see a larger overall picture of the network, and it lets you take actions on multiple systems or network resources if an attack is under way. Such a centralized area is called a *network operations center (NOC)*. Using a NOC makes it easier to see how an attack develops and to provide countermeasures. Unfortunately, a NOC is beyond the means of most medium-sized and small businesses. NOCs are expensive and require a great deal of support: factors beyond the economy or scale of all but the largest businesses. After a NOC is developed and implemented, the job doesn't stop there—the NOC must be constantly evaluated and changed as needed.

If your organization does not employ a dedicated security professional but you still need to implement security measures, one approach is to outsource to a *managed security service provider (MSSP)*. MSSPs offer overall security services to small companies and can be more cost effective than adding a dedicated individual to the payroll.

AT&T Wireless NOCs

AT&T Wireless maintains a huge NOC for each of the cell centers it manages. These centers provide 24/7 real-time monitoring of all devices in the cellular and computer network they support. The operators in the NOC can literally reach out and touch any device in the network to configure, repair, and troubleshoot it. A single NOC has dozens of people working around the clock to keep on top of the network. When an AT&T Wireless center goes down, it effectively takes down the cell-phone service for an entire region. As you can imagine, this is horrendously expensive, and the company doesn't let it happen often. There are several NOC facilities in the United States, and one region can support or take over operations for another region if that center becomes inoperable.

Understanding the Different Network Infrastructure Devices

Connecting all these components requires physical devices. Large multinational corporations, as well as small and medium-sized corporations, are building networks of enormous complexity and sophistication. These networks work by utilizing miles of both wiring and *wireless technologies*. If the network is totally wire and fiber based or totally wireless, the method of transmitting data from one place to another opens vulnerabilities and opportunities for exploitation. Vulnerabilities appear whenever an opportunity exists to intercept information from the media.

The devices briefly described here are the components you'll typically encounter in a network.

Many network devices contain firmware that you interact with during configuration. For security purposes, you must authenticate in order to make configuration changes and do so initially by using the default account(s). Make sure the default password is changed after the installation on any network device; otherwise you are leaving that device open for anyone recognizing the hardware to access it using the known factory password.

Firewalls

Firewalls are one of the first lines of defense in a network. There are different types of firewalls, and they can be either stand-alone systems or included in other devices such as routers or servers. You can find firewall solutions that are marketed as hardware only and

others that are software only. Many firewalls, however, consist of add-in software that is available for servers or workstations.

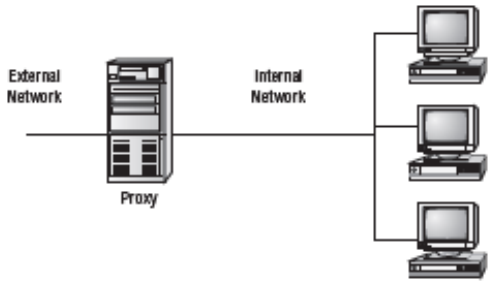
Although solutions are sold as "hardware only," the hardware still runs some sort of software. It may be hardened and in ROM to prevent tampering, and it may be customized—but software is present nonetheless.

The basic purpose of a firewall is to isolate one network from another. Firewalls are becoming available as appliances, meaning they're installed as the primary device separating two networks. *Appliances* are freestanding devices that operate in a largely self-contained manner, requiring less maintenance and support than a server-based product.

To understand the concept of a firewall, it helps to know where the term comes from. In days of old, dwellings used to be built so close together that if a fire broke out in one, it could easily destroy a block or more before it could be contained. To decrease the risk of this happening, firewalls were built between buildings. The firewalls were huge brick walls that separated the buildings and kept a fire confined to one side. The same concept of restricting and confining is true in network firewalls. Traffic from the outside world hits the firewall and isn't allowed to enter the network unless otherwise invited.

The firewall shown in Figure 2.14 effectively limits access from outside networks, while allowing inside network users to access outside resources. The firewall in this illustration is also performing proxy functions, discussed later.

FIGURE 2.14 A proxy firewall blocking network access from external networks



Firewalls function as one or more of the following:

- Packet filter
- Proxy firewall
- Stateful inspection firewall

Although firewalls are often associated with outside traffic, you can place a firewall anywhere. For example, if you want to isolate one portion of your internal network from others, you can place a firewall between them.

Packet Filter Firewalls

A firewall operating as a *packet filter* passes or blocks traffic to specific addresses based on the type of application. The packet filter doesn't analyze the data of a packet; it decides whether to pass it based on the packet's addressing information. For instance, a packet filter may allow web traffic on port 80 and block Telnet traffic on port 23. This type of filtering is included in many routers. If a received packet request asks for a port that isn't authorized, the filter may reject the request or simply ignore it. Many packet filters can also specify which IP addresses can request which ports and allow or deny them based on the security settings of the firewall.

Packet filters are growing in sophistication and capability. A packet filter firewall can allow any traffic that you specify as acceptable. For example, if you want web users to access your site, then you configure the packet filter firewall to allow data on port 80 to enter. If every network were exactly the same, firewalls would come with default port settings hard-coded, but networks vary, so the firewalls don't include such settings.

Decide Which Traffic to Allow Through

As an administrator, you need to survey your network and decide which traffic should be allowed through the firewall. What traffic will you allow in, and what will you block at the firewall?

The following is a list of only the most common TCP ports. Check the boxes indicating whether you'll allow data using this port through the firewall.

TCP Port Number	Service	Yes	No
20	FTP (data channel)	❑	❑
21	FTP (control channel)	❑	❑
23	Telnet	❑	❑
25	SMTP	❑	❑
49	TACACS authentication service	❑	❑
80	HTTP (used for World Wide Web)	❑	❑

TCP Port Number	Service	Yes	No
110	POP3	❑	❑
119	NNTP	❑	❑
137, 138, and 139	NetBIOS session service	❑	❑
143	IMAP	❑	❑
389	LDAP	❑	❑
443	HTTPS (used for secure web connections)	❑	❑
636	LDAP (SSL)	❑	❑

Proxy Firewalls

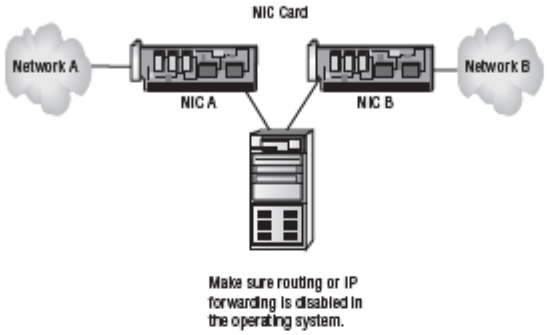
A *proxy firewall* can be thought of as an intermediary between your network and any other network. Proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rule-based decisions about whether the request should be forwarded or refused. The proxy intercepts all the packages and reprocesses them for use internally. This process includes hiding IP addresses.

When you consider the concept of hiding IP addresses, think of Network Address Translation (NAT) as it is discussed in the section "Working with Newer Technologies."

The proxy firewall provides better security than packet filtering because of the increased intelligence that a proxy firewall offers. Requests from internal network users are routed through the proxy. The proxy, in turn, repackages the request and sends it along, thereby isolating the user from the external network. The proxy can also offer caching, should the same request be made again, and can increase the efficiency of data delivery.

A proxy firewall typically uses two network interface cards (NICs). This type of firewall is referred to as a *dual-homed firewall*. One of the cards is connected to the outside network, and the other is connected to the internal network. The proxy software manages the connection between the two NICs. This setup segregates the two networks from each other and offers increased security. Figure 2.15 illustrates a dual-homed firewall segregating two networks from each other.

FIGURE 2.15 A dual-homed firewall segregating two networks from each other



Real World Scenario

Dual-Homed Proxy Firewall

You're the network administrator of a small network. You're installing a new firewall server. After you complete the installation, you notice that the network doesn't appear to be routing traffic through the firewall and that inbound requests aren't being blocked. This situation presents a security problem for the network because you've been getting unusual network traffic lately.

The most likely solution to this problem deals with the fact that the server offers the ability to use IP forwarding in a dual-homed server. IP forwarding bypasses your firewall and uses the server as a router. Even though the two networks are effectively isolated, the new router is doing its job well, and it's routing IP traffic.

You'll need to verify that IP forwarding and routing services aren't running on this server.

Anytime you have a system that is configured with more than one IP address, it can be said to be *multihomed*.

The proxy function can occur at either the application level or the circuit level.

Application-level proxy functions read the individual commands of the protocols that are being served. This type of server is advanced and must know the rules and capabilities of the protocol used. An implementation of this type of proxy must know the difference between GET and PUT operations, for example, and have rules specifying how to execute them. A *circuit-level proxy* creates a circuit between the client and the server and doesn't deal with the contents of the packets that are being processed.

A unique application-level proxy server must exist for each protocol supported. Many proxy servers also provide full *auditing*, *accounting*, and other usage information that wouldn't normally be kept by a circuit-level proxy server.

Stateful Inspection Firewalls

The last section on firewalls focuses on the concept of stateful inspection. In order to understand the terminology, it helps to know that what came before was referred to as *stateless*. Stateless firewalls make decisions based on the data that comes in—the packet, for example—and not based on any complex decisions.

Stateful inspection is also referred to as *stateful packet filtering*. Most of the devices used in networks don't keep track of how information is routed or used. After a packet is passed, the packet and path are forgotten. In stateful inspection (or stateful packet filtering), records are kept using a state table that tracks every communications channel. Stateful inspections occur at all levels of the network and provide additional security, especially in connectionless protocols such as User Datagram Protocol and Internet Control Message Protocol. This adds complexity to the process. Denial-of-Service attacks present a challenge because flooding techniques are used to overload the state table and effectively cause the firewall to shut down or reboot.

For the exam, remember that pure packet filtering has no real intelligence. It allows data to pass through a port if that port is configured and otherwise discards it—it doesn't examine the packets. Stateful packet filtering, however, has intelligence in that it keeps track of every communications channel.

Hubs

One of the simplest devices in a network is a hub. Although it's possible to load software to create a managed hub, in its truest sense, a *hub* is nothing more than a device allowing many hosts to communicate with each other through the use of physical ports. Broadcast traffic can traverse the hub, and all data received through one port is sent to all other ports. This arrangement creates an extremely unsecure environment should an intruder attach to a hub and begin intercepting data.

Broadcasts are messages sent from a single system to the entire network. *Multicasting* sends a message to multiple addresses. *Unicasts* are oriented at a single system.

Some of the more expensive hubs do allow you to enable *port security*. If this is enabled, each port takes note of the first MAC address it hears on that port. If the MAC address changes, the hub disables the port. Port security increases the level of security on the LAN, but it can also increase the administrator's workload if you reconfigure your environment often.

For exam purposes, think of hubs as, by default, being unsecure LAN devices that should be replaced with switches for security and increased throughput.

Modems

A *modem* is a hardware device that connects the digital signals from a computer to an analog telephone line. It allows the signals to be transmitted over longer distances than are normally possible. The word *modem* is an amalgam of the words *modulator* and *demodulator*, which are the two functions that occur during transmission.

Modems present a unique set of challenges from a security perspective. Most modems answer any call made to them when connected to an outside line. After the receiving modem answers the phone, it generally synchronizes with a caller's modem and makes a connection. A modem, when improperly connected to a network, can allow instant unsecured access to the system's or network's data and resources. If a physical security breach occurs, a modem can be used as a remote network connection that allows unrestricted access. This can occur with no knowledge on the part of the system's owner or the network administrators.

While modems are not used as much as they once were, many PCs being built and delivered today still come with internal modems. Unless the modems are specifically needed, they should be disabled or removed from network workstations. If this isn't possible, they should be configured not to auto-answer incoming calls. In other words, you must eliminate as many features of the modem as possible in order to increase security.

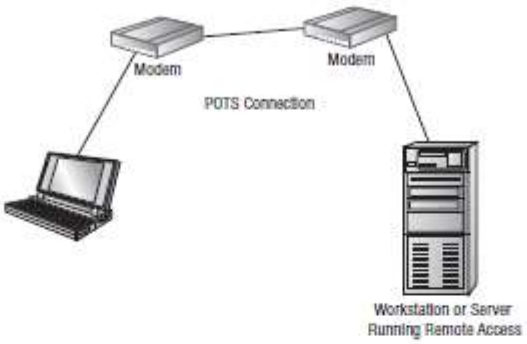
Many preconfigured administrative systems provide modem connections for remote maintenance and diagnostics. These connections should either be password protected or have a cut-off switch so they don't expose your network to security breaches.

Remote Access Services

Remote Access Services (RAS) refers to any server service that offers the ability to connect remote systems. The current Microsoft product for Windows-based clients is called *Routing and Remote Access Services (RRAS)*, but it was previously known as Remote Access Services (RAS). Because of this, you'll encounter the term *RAS* used interchangeably to describe both the Microsoft product and the process of connecting to remote systems.

Figure 2.16 depicts a dial-up connection being made from a workstation to a network using a RAS server on the network. In this case, the connection is being made between a Windows-based system and a Windows server using *plain-old telephone service (POTS)* and a modem.

FIGURE 2.16 A RAS connection between a remote workstation and a Windows server



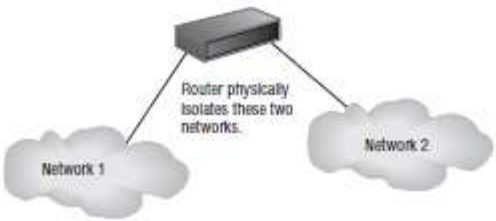
The RAS connection is accomplished via dial-up or network technologies such as VPNs, ISDN, DSL, and cable modems. RAS connections may be secure or in the clear, depending on the protocols that are used in the connection.

A popular method of remote access is through the use of PC Anywhere and similar remote connection/virtual network programs. A major issue with Virtual Network Computing (VNC) is that you are leaving a door into the network open that anyone may stumble upon. By default, most of these programs start the server service automatically, and it is running even when it is not truly needed. It is highly recommended that you configure the service as a manual start service and launch it *only* when needed to access the host. At all other times, that service should be shut down.

Routers

The primary instrument used for connectivity between two or more networks is the *router*. Routers work by providing a path between the networks. A router has two connections that are used to join the networks. Each connection has its own address and appears as a valid address in its respective network. Figure 2.17 illustrates a router connected between two LANs.

FIGURE 2.17 Router connecting two LANs



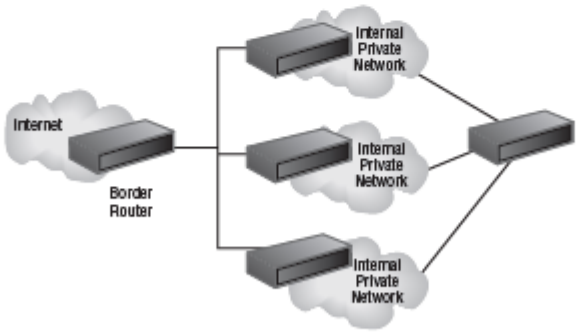
Routers are intelligent devices, and they store information about the networks to which they're connected. Most routers can be configured to operate as packet-filtering firewalls. Many of the newer routers also provide advanced firewall functions.

Routers, in conjunction with a Channel Service Unit/Data Service Unit (CSU/DSU), are also used to translate from *LAN framing* to *WAN framing* (for example, a router that connects a 100BaseT network to a T1 network). This is needed because the network protocols are different in LANs and WANs. Such routers are referred to as *border routers*. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network. Like the border patrols of many countries, border routers decide who can come in and under what conditions.

Dividing internal networks into two or more subnetworks is a common use for routers. Routers can also be connected internally to other routers, effectively creating *zones* that operate autonomously. Figure 2.18 illustrates a corporate network that uses the combination of a border router for connection to an ISP and internal routers to create autonomous networks for communications. This type of connection keeps local network traffic off the backbone of the corporate network and provides additional security to internal users.

Because broadcasts don't traverse routers, network segmentation decreases traffic.

FIGURE 2.18 A corporate network implementing routers for segmentation and security



Routers establish communication by maintaining tables about destinations and local connections. A router contains information about the systems connected to it and where to send requests if the destination isn't known. These tables grow as connections are made through the router.

Routers usually communicate routing and other information using one of three standard protocols. Routing can occur interior to the network or exterior, and the three protocols in question are defined here:

Routing Information Protocol (RIP) RIP is a simple protocol that is part of the TCP/IP protocol suite. Routers that use RIP routinely broadcast the status and routing information of known routers. RIP also attempts to find routes between systems using the smallest number of hops or connections. Multiple versions of RIP are available, with version 2 being the most used today.

Border Gateway Protocol (BGP) BGP allows groups of routers to share routing information.

Open Shortest Path First (OSPF) OSPF allows routing information to be updated faster than with RIP.

In the Cisco world, *Interior Gateway Routing Protocol (IGRP)* and *Enhanced Interior Gateway Routing Protocol (EIGRP)* are commonly used. These are distance vector protocols that automatically/mathematically compute routes and choose the best one.

Routers are your first line of defense, and they must be configured to pass only traffic that is authorized by the network administrators. In effect, a router can function as a firewall if it's configured properly. The best approach is layered; a router shouldn't take the place of a firewall but simply augment it.

The routes themselves can be configured as static or dynamic. If they are static, then they are edited manually and stay that way until changed. If they are dynamic, then they learn of other routers around them and use information about those to build their routing tables.

Switches

Switches are multiport devices that improve network efficiency. A switch typically has a small amount of information about systems in a network. Using switches improves network efficiency over hubs because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. You can think of a switch as a device that has some of the best capabilities of routers and hubs combined.

The switch maintains limited routing information about systems in the internal network and allows connections to systems like a hub. Figure 2.19 shows a switch in action between two workstations in a LAN. The connection isn't usually secure or encrypted; however, it doesn't leave the switched area and become part of the overall broadcast traffic as typically happens on a star-based or bus-based LAN.

FIGURE 2.19 Switching between two systems

Load Balancers

Load balancing refers to shifting a load from one device to another. Most often the device in question is a server, but the term could be used for a hard drive, a CPU, or almost any device that you want to avoid overloading. Using a server as the device in question, balancing the load between multiple servers instead of relying on only one reduces the response time, maximizes throughput, and allows better allocation of resources.

A *load balancer* can be implemented as a software or hardware solution and is usually associated with a device—a router, a firewall, NAT, and so on. Under the most common implementation, the load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available (if a server that should be available is busy or down, it is taken out of the rotation).

Telecom/PBX Systems

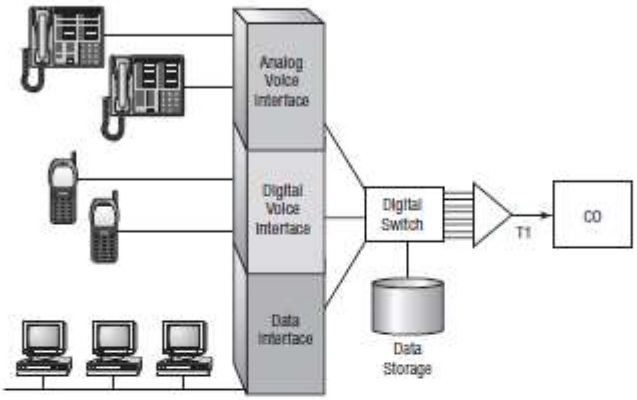
Telecommunications (or *telecom*) capabilities have undergone radical changes in the last 10 years. The telephone systems and technologies available to deal with communications have given many small businesses fully integrated voice and data services at reasonable prices.

These changes have complicated the security issues that must be handled. One of the primary tools in communications systems is the *private branch exchange (PBX)* system. PBX systems now allow users to connect voice, data, pagers, networks, and almost any other conceivable application into a single telecommunications system. In short, a PBX system allows a company to be its own phone company.

The technology is developing to the point where all communications occur via data links to phone companies using standard data transmission technologies, such as T1 or T3. This means that both voice and data communications are occurring over the same network connection to a phone company or a provider. This allows a single connection for all communications to a single provider of these services.

Potentially, your phone system is a target for attack. Figure 2.20 shows a PBX system connected to a phone company using a T1 line. The phone company, in this illustration, is abbreviated CO (for central office). The phone company systems that deal with routing and switching of calls and services are located at the CO.

FIGURE 2.20 A modern digital PBX system integrating voice and data onto a single network connection



If your phone system is part of your data communications network, an attack on your network will bring down your phone system. This event can cause the stress level in a busy office to increase dramatically.

Find the Holes

The United States Department of Commerce, in conjunction with the National Institute of Standards and Technology, has posted an excellent article titled "PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does" at `http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf`. This document walks through system architecture, hardware, maintenance, and other issues relevant to daily administration as well as exam study.

The security problems in this situation also increase because you must work to ensure security for your voice communications. At the time the exam questions were written, there were no incidents you needed to be aware of involving phone systems being attacked by malicious code. Since then, some Voice over IP attacks have been reported, and such attacks will probably become a greater concern in the near future.

For the exam, know that because a PBX has many of the same features as other network components, it's subject to the same issues, such as leaving TCP ports open. The PBX should be subject to audit and monitoring like every other network component.

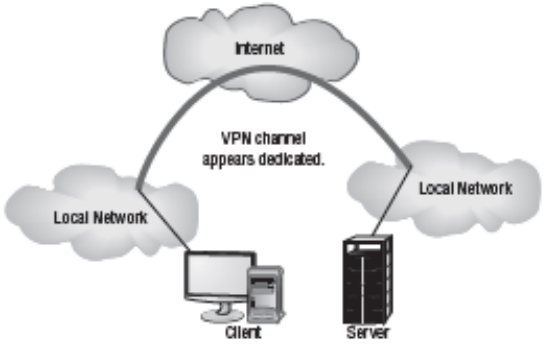
Imagine that someone left a voice message for the president of your company. A *phreaker* (someone who abuses phone systems, as opposed to data systems) might intercept this message, alter it, and put it back. The result of this prank could be a calamity for the company (or at least for you). Make sure the default password is changed on the maintenance and systems accounts for a PBX after its installation, as you would for any network device.

Virtual Private Networks

A *virtual private network (VPN)* is a private network connection that occurs through a public network. A private network provides security over an otherwise unsecure environment. VPNs can be used to connect LANs together across the Internet or other public networks. With a VPN, the remote end appears to be connected to the network as if it were connected locally. A VPN requires either special hardware to be installed or a VPN software package running on servers and workstations.

VPNs typically use a tunneling protocol such as Layer 2 Tunneling Protocol, IPSec, or Point-to-Point Tunneling Protocol (PPTP). Figure 2.21 shows a remote network being connected to a LAN using the Internet and a VPN. This connection appears to be a local connection, and all message traffic and protocols are available across the VPN.

FIGURE 2.21 Two LANs being connected using a VPN across the Internet



VPNs are becoming the connection of choice when establishing an extranet or intranet between two or more remote offices. The major security concern when using a VPN is encryption. PPTP offers some encryption capabilities, although they're weak. IPSec

offers higher security, and it's becoming the encryption system used in many secure VPN environments.

Even though a VPN is created through the Internet or other public network, the connection logically appears to be part of the local network. This is why a VPN connection used to establish a connection between two private networks across the Internet is considered a private connection or an extranet.

As mentioned earlier, VPNs are used to make connections between private networks across a public network, such as the Internet. These connections aren't guaranteed to be secure unless a tunneling protocol (such as PPTP) and an encryption system (such as IPSec) are used. A wide range of options, including proprietary technologies, is available for VPN support. Many of the large ISPs and data communications providers offer dedicated hardware with VPN capabilities. Many servers also provide software VPN capabilities for use between two networks.

VPN systems can be dedicated to a certain protocol, or they can pass whatever protocols they see on one end of the network to the other end. A pure VPN connection appears as a dedicated wired connection between the two network ends.

A *VPN concentrator* is a hardware device used to create remote access VPNs. The concentrator creates encrypted tunnel sessions between hosts, and many use two-factor authentication for additional security. Cisco models often incorporate *Scalable Encryption Processing (SEP)* modules to allow for hardware-based encryption and/or redundancy.

Web Security Gateway

One of the newest buzzwords is *web security gateway*, which can be thought of as a proxy server (performing proxy and caching functions) with web protection software built in. Depending on the vendor, the "web protection" can range from a standard virus scanner on incoming packets to also monitoring outgoing user traffic for red flags.

Potential red flags the gateway can detect/prohibit include inappropriate content, trying to establish a peer-to-peer connection with a file-sharing site, instant messaging, and unauthorized tunneling. You can configure most web security gateways to block known HTTP/HTML exploits, strip ActiveX tags, strip Java applets, and block/strip cookies.

Spam Filters

Spam filters can be added to catch unwanted email and filter it out before it gets delivered internally. The filtering is done based on rules that are established (block email coming from certain IP addresses, email that contains particular words in the subject line, and the like).While spam filters are usually used to scan incoming messages, they can also be used to scan outgoing as well and thus act as a quick identifier of internal PCs that may have contracted a virus.

It is estimated that over 90 percent of the incoming email to many organizations is spam. SpamAssassin is one of the best known open source spam filters, and you can find more information on it at `http://spamassassin.apache.org/`.

A number of vendors make all-in-one security devices that combine spam filters with firewalls, load balancers, and a number of other services.

Understanding Remote Access

One of the primary purposes for having a network is the ability to connect systems. As networks have grown, many technologies have come on the scene to make this process easier and more secure. A key area of concern relates to the connection of systems and other networks that aren't part of your network. The following sections discuss the more common protocols used to facilitate connectivity among remote systems.

Any authentication done for a remote user is known as *remote authentication*. This authentication is commonly done using TACACS or RADIUS (which are discussed in Chapter 5).

Using Point-to-Point Protocol

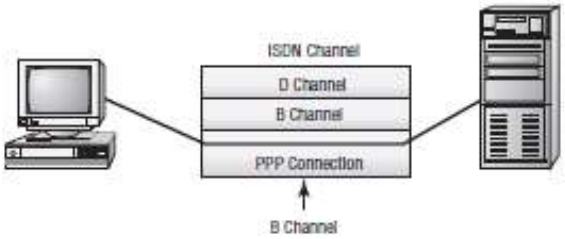
Introduced in 1994, *Point-to-Point Protocol (PPP)* offers support for multiple protocols including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP doesn't provide data security, but it does provide authentication using *Challenge Handshake Authentication Protocol (CHAP)*.

Figure 2.22 shows a PPP connection over an ISDN line. In the case of ISDN, PPP would normally use one 64Kbps B channel for transmission. PPP allows many channels in a network connection (such as ISDN) to be connected or bonded together to form a single virtual connection.

PPP works by encapsulating the network traffic in a protocol called *Network Control Protocol (NCP)*. Authentication is handled by *Link Control Protocol (LCP)*. A PPP connection allows remote users to log on to the network and have access as though they were local users on the network. PPP doesn't provide for any encryption services for the channel.

As you might have guessed, the unsecure nature of PPP makes it largely unsuitable for WAN connections. To counter this issue, other protocols have been created that take advantage of PPP's flexibility and build on it. A dial-up connection using PPP works well because it isn't common for an attacker to tap a phone line. You should make sure all your PPP connections use secure channels, dedicated connections, or dial-up connections.

FIGURE 2.22 PPP using a single B channel on an ISDN connection



Remote users who connect directly to a system using dial-up connections don't necessarily need to have encryption capabilities enabled. If the connection is direct, the likelihood that anyone would be able to tap an existing phone line is relatively small. However, you should make sure that connections through a network use an encryption-oriented tunneling system.

Working with Tunneling Protocols

Tunneling protocols add a capability to the network: the ability to create tunnels between networks that can be more secure, support additional protocols, and provide virtual paths between systems. The best way to think of tunneling is to imagine sensitive data being encapsulated in other packets that are sent across the public network. Once they're received at the other end, the sensitive data is stripped from the other packets and recompiled into its original form.

The most common protocols used for tunneling are as follows:

Point-to-Point Tunneling Protocol *Point-to-Point Tunneling Protocol (PPTP)* supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. After the negotiation is performed, the channel is encrypted. This is one of the major weaknesses of PPTP. A *packet-capture device*, such as a sniffer, that captures the negotiation process can potentially use that information to determine the connection type and information about how the tunnel works. Microsoft developed PPTP and supports it on most of the company's products. PPTP uses port 1723 and TCP for connections.

Layer 2 Forwarding *Layer 2 Forwarding (L2F)* was created by Cisco as a method of creating tunnels primarily for dial-up connections. It's similar in capability to PPP and shouldn't be used over WANs. L2F provides authentication, but it doesn't provide encryption. L2F uses port 1701 and TCP for connections.

Layer 2 Tunneling Protocol Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: *Layer 2 Tunneling Protocol (L2TP)*. L2TP is a hybrid of PPTP and L2F. It's primarily a point-to-point protocol. L2TP supports multiple

network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP, so it can be used as a bridge across many types of systems. The major problem with L2TP is that it doesn't provide data security: The information isn't encrypted. Security can be provided by protocols such as IPSec. L2TP uses port 1701 and UDP for connections.

Secure Shell *Secure Shell (SSH)* is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent programs for such Unix standards as Telnet, FTP, and many other communications-oriented applications. SSH is now available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext-oriented programs in the Unix environment. SSH uses port 22 and TCP for connections.

Internet Protocol Security *Internet Protocol Security (IPSec)* isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with dial-up connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security. IPSec can work in either Tunneling mode or Transport mode. In Tunneling mode, the data or payload and message headers are encrypted. Transport mode encrypts only the payload.

Real World Scenario

Connecting Remote Network Users

Your company wants to support network connections for remote users. These users will use the Internet to access desktop systems and other resources in the network. What would you advise the company to consider?

You should advise your organization to implement a tunneling protocol that supports security. A good solution would be a VPN connection that uses IPSec. You might also want to explore protocols like SSL, TLS, and SSH as alternatives. All of these protocols offer security as a part of their connection process.

Summary

In this chapter, I covered the key elements of the network infrastructure and the various components involved in networking. Your infrastructure is the backbone and key to all the security capabilities of your network.

Your infrastructure includes the hardware and software necessary to run your network. The key elements used in security are routers and firewalls. Proper configuration is the key to providing services the way your network needs them. If your network security devices

are improperly configured, you may be worse off than if you didn't have them at all. It's a dangerous situation when you think you're secure but in actuality you aren't.

Networks are becoming more complicated, and they're being linked to other networks at an accelerated speed. Several tools are available to help you both link and secure your networks:

- VPNs
- Tunneling protocols
- Remote access

The connections you make using TCP/IP are based primarily on IP addresses. When coupled with a port, these addresses form a socket. Sockets are the primary method used to communicate with services and applications such as the Web and Telnet. Most services have standard sockets that operate by default. Sockets are changeable for special configurations and additional security. Changing default ports requires that users know which ports provide which services.

Exam Essentials

Be able to describe the various components and the purpose of an infrastructure. Your network's infrastructure is the backbone of your systems and network operations. The infrastructure includes all the hardware, software, physical security, and operational security methods in place. The key components of your infrastructure include devices such as routers, firewalls, switches, modems, telecommunications systems, and the other devices used in the network.

Know the characteristics of the connectivity technologies available to you and the security capabilities associated with each. Remote access, PPP, tunneling protocols, and VPNs are your primary tools. PPTP and L2TP are two of the most common protocols used for tunneling. IPSec, although not a tunneling protocol, provides encryption to tunneling protocols; it's often used to enhance tunnel security.

Familiarize yourself with the technologies used by TCP/IP and the Internet. IP addresses and port numbers are combined to create an interface called a socket. Most TCP and UDP protocols communicate using this socket as the primary interface mechanism. Clients and servers communicate using ports. Ports can be changed to enhance security. Web services use HTML and other technologies to allow rich and animated websites. These technologies potentially create security problems because they may have individual vulnerabilities. Verify the problems that exist from a security perspective before enabling these technologies on your systems.

Review Questions

1. Which of the following devices is the most capable of providing infrastructure security?
   - **A.** Hub
   - **B.** Switch
   - **C.** Router
   - **D.** Modem
2. Upper management has decreed that a firewall must be put in place immediately, before your site suffers an attack similar to one that struck a sister company. Responding to this order, your boss instructs you to implement a packet filter by the end of the week. A packet filter performs which function?
   - **A.** Prevents unauthorized packets from entering the network
   - **B.** Allows all packets to leave the network
   - **C.** Allows all packets to enter the network
   - **D.** Eliminates collisions in the network
3. Which device stores information about destinations in a network?
   - **A.** Hub
   - **B.** Modem
   - **C.** Firewall
   - **D.** Router
4. As more and more clients have been added to your network, the efficiency of the network has decreased significantly. You're preparing a budget for next year, and you specifically want to address this problem. Which of the following devices acts primarily as a tool to improve network efficiency?
   - **A.** Hub
   - **B.** Switch
   - **C.** Router
   - **D.** PBX
5. Which device is used to connect voice, data, pagers, networks, and almost any other conceivable application into a single telecommunications system?
   - **A.** Router
   - **B.** PBX
   - **C.** Hub
   - **D.** Server

6. Most of the sales force have been told that they should no longer report to the office on a daily basis. From now on, they're to spend the majority of their time on the road calling on customers. Each member of the sales force has been issued a laptop computer and told to connect to the network nightly through a dial-up connection. Which of the following protocols is widely used today as a transport protocol for Internet dial-up connections?
   A. SMTP
   B. PPP
   C. PPTP
   D. L2TP

7. Which protocol is unsuitable for WAN VPN connections?
   A. PPP
   B. PPTP
   C. L2TP
   D. IPSec

8. You've been given notice that you'll soon be transferred to another site. Before you leave, you're to audit the network and document everything in use and the reason why it's in use. The next administrator will use this documentation to keep the network running. Which of the following protocols isn't a tunneling protocol but is probably used at your site by tunneling protocols for network security?
   A. IPSec
   B. PPTP
   C. L2TP
   D. L2F

9. A socket is a combination of which components?
   A. TCP and port number
   B. UDP and port number
   C. IP and session number
   D. IP and port number

10. You're explaining protocols to a junior administrator shortly before you leave for vacation. The topic of Internet mail applications comes up, and you explain how communications are done now as well as how you expect them to be done in the future. Which of the following protocols is becoming the newest standard for Internet mail applications?
    A. SMTP
    B. POP
    C. IMAP
    D. IGMP

11. Which protocol is primarily used for network maintenance and destination information?
    A. ICMP
    B. SMTP
    C. IGMP
    D. Router

12. You're the administrator for Mercury Technical. A check of protocols in use on your server brings up one that you weren't aware was in use; you suspect that someone in HR is using it to send messages to multiple recipients. Which of the following protocols is used for group messages or multicast messaging?
    A. SMTP
    B. SNMP
    C. IGMP
    D. L2TP

13. IPv6, in addition to having more bits allocated for each host address, also has mandatory requirements built in for which security protocol?
    A. TFTP
    B. IPSec
    C. SFTP
    D. L2TP

14. Which ports are, by default, reserved for use by FTP? (Choose all that apply.)
    A. 20 and 21 TCP
    B. 20 and 21 UDP
    C. 22 and 23 TCP
    D. 22 and 23 UDP

15. Which of the following services use only TCP ports and not UDP? (Choose all that apply.)
    A. IMAP
    B. LDAP
    C. FTPS
    D. SFTP

16. Which of the following can be implemented as a software or hardware solution and is usually associated with a device—a router, a firewall, NAT, and so on—and used to shift a load from one device to another?
    A. Proxy
    B. Hub
    C. Load balancer
    D. Switch

17. Which of the following are multiport devices that improve network efficiency?
    A. Switches
    B. Modems
    C. Gateways
    D. Concentrators
18. Which service(s), by default, use TCP and UDP port 22? (Choose all that apply.)
    A. SMTP
    B. SSH
    C. SCP
    D. IMAP
19. What protocol, running on top of TCP/IP, is often used for name registration and resolution with Windows-based clients?
    A. Telnet
    B. SSL
    C. NetBIOS
    D. TLS
20. How many bits are used for addressing with IPv4 and IPv6, respectively?
    A. 32, 128
    B. 16, 64
    C. 8, 32
    D. 4, 16

Answers to Review Questions

1. C. Routers can be configured in many instances to act as packet-filtering firewalls. When configured properly, they can prevent unauthorized ports from being opened.
2. A. Packet filters prevent unauthorized packets from entering or leaving a network. Packet filters are a type of firewall that blocks specified port traffic.
3. D. Routers store information about network destinations in routing tables. Routing tables contain information about known hosts on both sides of the router.
4. B. Switches create virtual circuits between systems in a network. These virtual circuits are somewhat private and reduce network traffic when used.
5. B. Many modern PBX (private branch exchange) systems integrate voice and data onto a single data connection to your phone service provider. In some cases, this allows an overall reduction in cost of operations. These connections are made using existing network connections such as a T1 or T3 network.
6. B. PPP can pass multiple protocols and is widely used today as a transport protocol for dial-up connections.
7. A. PPP provides no security, and all activities are unsecure. PPP is primarily intended for dial-up connections and should never be used for VPN connections.
8. A. IPSec provides network security for tunneling protocols. IPSec can be used with many different protocols besides TCP/IP, and it has two modes of security.
9. D. A socket is a combination of IP address and port number. The socket identifies which application will respond to the network request.
10. C. IMAP is becoming the most popular standard for email clients and is replacing POP protocols for mail systems. IMAP allows mail to be forwarded and stored in information areas called stores.
11. A. ICMP is used for destination and error reporting functions in TCP/IP. ICMP is routable and is used by programs such as Ping and Traceroute.
12. C. IGMP is used for group messaging and multicasting. IGMP maintains a list of systems that belong to a message group. When a message is sent to a particular group, each system receives an individual copy.
13. B. The implementation of IPSec is mandatory with IPv6. While it is widely implemented with IPv4, it is not a requirement.
14. A. FTP uses TCP ports 20 and 21. FTP does not use UDP ports.
15. D. SFTP uses only TCP ports. IMAP, LDAP, and FTPS all use both TCP and UDP ports.

16. C. A load balancer can be implemented as a software or hardware solution, and is usually associated with a device—a router, a firewall, NAT, and so on. As the name implies, it is used to shift a load from one device to another.

17. A. Switches are multiport devices that improve network efficiency. A switch typically has a small amount of information about systems in a network.

18. B, C. Port 22 is used by both SSH and SCP with TCP and UDP.

19. C. NetBIOS is used for name resolution and registration in Windows-based environments. It runs on top of TCP/IP.

20. A. IPv4 uses 32 bits for the host address, while IPv6 uses 128 bits for this.

Chapter 3: Protecting Networks

Protecting Networks

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **3.1 Explain the security function and purpose of network devices and technologies.**
  - NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic)
  - Protocol analyzers
  - Sniffers
- ✓ **3.5 Analyze and differentiate among types of application attacks.**
  - Cross-site scripting
  - Buffer overflow
  - Cookies and attachments
  - Malicious add-ons
- ✓ **3.6 Analyze and differentiate among types of mitigation and deterrent techniques.**
  - Detection controls vs. prevention controls
    - IDS vs. IPS
- ✓ **3.7 Implement assessment tools and techniques to discover security threats and vulnerabilities.**
  - Tools
    - Protocol analyzer
    - Sniffer
    - Honeypots
    - Honeynets
    - Port scanner

- ✓ **4.1 Explain the importance of application security.**
  - Secure coding concepts
    - Error and exception handling
    - Input validation
  - Cross-site scripting prevention

While the first chapter looked at various forms of risk and how to calculate them, the second chapter looked at the technology the network is built upon and some devices that can help mitigate some of the risk. The focus of this chapter is on identifying security-related problems when they do occur.

Intrusion detection and intrusion prevention, whether network based or local, provide key methods of identifying intrusions and notifying administrators when responses are needed. In addition to these monitors, you can create traps for those who violate security, by building honeypots and honeynets that fool the intruders and allow you to track them or catch them.

Lastly, this chapter looks at some of the key concepts in application security and problems to be aware of.

Monitoring and Diagnosing Networks

It is important to monitor the network and make sure the traffic on it belongs there. In this section, we'll explore basic network monitors as well as intrusion detection systems.

Network Monitors

Network monitors, otherwise called *sniffers*, were originally introduced to help troubleshoot network problems. Simple network configuration programs like IPCONFIG don't get down on the wire and tell you what is physically happening on a network. Instead, examining the signaling and traffic that occurs on a network requires a network monitor. Early monitors were bulky and required a great deal of expertise to use. Like most things in the computer age, they have gotten simpler, smaller, and less expensive. Network monitors are now available for most environments, and they're effective and easy to use.

Today, a network-monitoring system usually consists of a PC with a NIC (running in *promiscuous mode*) and monitoring software. The monitoring software is menu driven, is easy to use, and has a big help file. The traffic displayed by sniffers can become overly involved and require additional technical materials; you can buy these materials at most bookstores, or you can find them on the Internet for free. With a few hours of work, most people can make network monitors work efficiently and use the data they present.

Windows Server products include a service called Network Monitor that you can use to gain basic information about network traffic. A more robust, detailed version of Network Monitor is included with Systems Management Server (SMS). When it comes to third-party products, Wireshark, available for most platforms, is a market leader (see `http://www.wireshark.org/` for more information).

Sniffer is a trade name, like Kleenex. It's the best-known network monitor, so everyone started calling network-monitoring hardware *sniffers*.

Intrusion Detection Systems

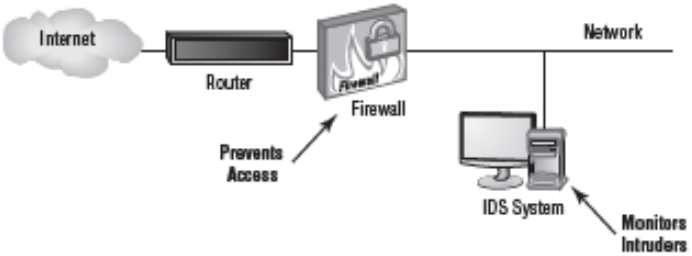
An intrusion detection system (IDS) is software that runs on either individual workstations or network devices to monitor and track network activity. By using an IDS, a network administrator can configure the system to respond just like a burglar alarm. IDSs can be configured to evaluate system logs, look at suspicious network activity, and disconnect sessions that appear to violate security settings.

Many vendors have oversold the simplicity of these tools. They're quite involved and require a great deal of planning and maintenance to work effectively. Many manufacturers are selling IDSs with firewalls, and this area shows great promise. Firewalls by themselves will prevent many common attacks, but they don't usually have the intelligence or the reporting capabilities to monitor the entire network. An IDS, in conjunction with a firewall, allows both a reactive posture with the firewall and a preventive posture with the IDS.

Figure 3.1 illustrates an IDS working in conjunction with a firewall to increase security.

In the event the firewall is compromised or penetrated, the IDS can react by disabling systems, ending sessions, and even potentially shutting down your network. This arrangement provides a higher level of security than either device provides by itself. A section exploring IDS in more detail appears later in this chapter.

FIGURE 3.1 An IDS and a firewall working together to secure a network



Understanding Intrusion Detection Systems

In the original *Walking Tall* movies, the sheriff puts small strips of clear tape on the hood of his car. Before getting in the vehicle, he would check the difficult-to-detect tape to see if it was broken—if it was, it tipped him off that someone had been messing beneath the hood, and that saved his life. Do you have clear tape on your network?

Intrusion detection systems (IDSs) are becoming integral parts of network monitoring. IDS is a relatively new technology, and it shows a lot of promise in helping to detect network intrusions. *Intrusion detection (ID)* is the process of monitoring events in a system or network to determine if an intrusion is occurring. An *intrusion* is defined as any activity or action that attempts to undermine or compromise the confidentiality, integrity, or availability of resources. Firewalls, as you may recall, were designed to prevent access to resources by an attacker. An IDS reports and monitors intrusion attempts.

Know the Resources Available in Linux

Security information is readily found at a number of Linux-related sites. The first to check, and stay abreast of, is always the distribution vendor's site. Its pages usually provide an overview of Linux-related security issues with links to other relevant pages. You should also keep abreast of issues and problems posted at `www.cert.org` and `www.linuxsecurity.com`.

You can also find information on any Linux command through a number of utilities inherent in Linux:

- The `man` tool offers pages on each utility. For example, to find information about the `setfacl` tool, you can type **`man setfacl`**.
- Most utilities have the built-in option of `-help` to offer information. From the command line, you can type **`setfacl --help`** to see a quick list of available options.
- The `info` utility shows the `man` pages as well.
- The `whatis` utility can show if there is more than one set of documentation on the system for the utility.
- The `whereis` utility lists all the information it can find about locations associated with a file.
- The `apropos` utility uses the `whatis` database to find values and returns the short summary information.

It should be inherently understood that every network, regardless of size, should utilize a firewall. On a home-based network, a personal software firewall can be implemented to provide protection against attacks.

Several key terms are necessary to explain the technology behind intrusion detection, as follows:

Activity An *activity* is an element of a data source that is of interest to the operator. This could include a specific occurrence of a type of activity that is suspicious. An example might be a TCP connection request that occurs repeatedly from the same IP address.

Administrator The *administrator* is the person responsible for setting the security policy for an organization and is responsible for making decisions about the deployment and configuration of the IDS. The administrator should make decisions regarding alarm levels, historical logging, and session-monitoring capabilities. They're also responsible for determining the appropriate responses to attacks and ensuring that those responses are carried out.

Most organizations have an escalation chart. The administrator is rarely at the top of the chart but is always expected to be the one doing the most to keep incidents under control.

Alert An *alert* is a message from the analyzer indicating that an event of interest has occurred. The alert contains information about the activity as well as specifics of the occurrence. An alert may be generated when an excessive amount of *Internet Control Message Protocol (ICMP)* traffic is occurring or when repeated logon attempts are failing. A certain level of traffic is normal for a network. Alerts occur when activities of a certain type exceed a preset threshold. For instance, you might want to generate an alert every time someone from inside your network pings the outside using the Ping program.

Analyzer The *analyzer* is the component or process that analyzes the data collected by the sensor. It looks for suspicious activity among all the data collected. Analyzers work by monitoring events and determining whether unusual activities are occurring, or they can use a rule-based process that is established when the IDS is configured.

Data Source The *data source* is the raw information that the IDS uses to detect suspicious activity. The data source may include audit files, system logs, or the network traffic as it occurs.

Event An *event* is an occurrence in a data source that indicates that a suspicious activity has occurred. It may generate an alert. Events are logged for future reference. They also typically trigger a notification that something unusual may be happening in the network. An IDS might begin logging events if the volume of inbound email connections suddenly spiked; this event might be an indication that someone was probing your network. The event might trigger an alert if a deviation from normal network traffic patterns occurred or if an activity threshold was crossed.

Manager The *manager* is the component or process the operator uses to manage the IDS. The IDS console is a manager. Configuration changes in the IDS are made by communicating with the IDS manager.

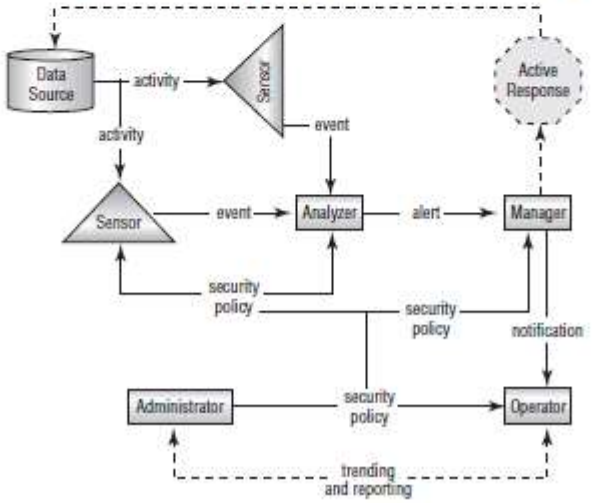
Notification *Notification* is the process or method by which the IDS manager makes the operator aware of an alert. This might include a graphic display highlighting the traffic or an email sent to the network's administrative staff.

Operator The *operator* is the person primarily responsible for the IDS. The operator can be a user, administrator, and so on, as long as they're the primary person responsible.

Sensor A *sensor* is the IDS component that collects data from the data source and passes it to the analyzer for analysis. A sensor can be a device driver on a system, or it can be an actual black box that is connected to the network and reports to the IDS. The important thing to remember is that the sensor is a primary data collection point for the IDS.

The IDS, as you can see, has many different components and processes that work together to provide a real-time picture of your network traffic. Figure 3.2 shows the various components and processes working together to provide an IDS. Remember that data can come from many different sources and must be analyzed to determine what's occurring. An IDS isn't intended as a true traffic-blocking device, though some IDSs can also perform this function; it's intended to be a traffic-auditing device.

FIGURE 3.2 The components of an IDS working together to provide network monitoring



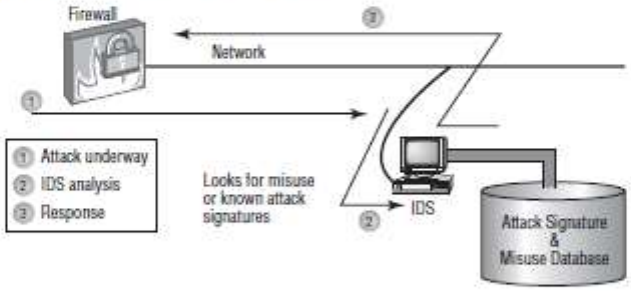
IDSs use four primary approaches:

Behavior-Based-Detection IDS A *behavior-based system* looks for variations in behavior such as unusually high traffic, policy violations, and so on. By looking for deviations in behavior, it is able to recognize potential threats and respond quickly.

Signature-Based-Detection IDS A *signature-based system*, also commonly known as *misuse-detection IDS (MD-IDS)*, is primarily focused on evaluating attacks based on attack signatures and audit trails. Attack signatures describe a generally established method of attacking a system. For example, a TCP flood attack begins with a large number of incomplete TCP sessions. If the MD-IDS knows what a TCP flood attack looks like, it can make an appropriate report or response to thwart the attack.

Figure 3.3 illustrates a signature-based IDS in action. Notice that this IDS uses an extensive database to determine the signature of the traffic. This process resembles an antivirus software process.

FIGURE 3.3 A signature-based IDS in action



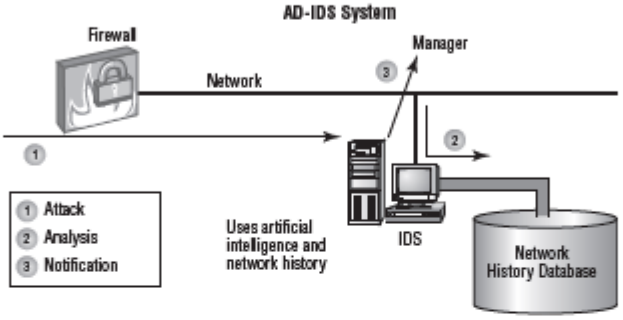
Anomaly-Detection IDS An *anomaly-detection IDS (AD-IDS)* looks for anomalies, meaning it looks for things outside of the ordinary. Typically, a training program learns what the normal operation is and then can spot deviations from it. An AD-IDS can establish the baseline either by being manually assigned values or through automated processes that look at traffic patterns. One method is *behavior-based*, which looks for unusual behavior and then acts accordingly.

Heuristic IDS A *heuristic system* uses algorithms to analyze the traffic passing through the network. As a general rule, heuristic systems require more tweaking and fine-tuning than the other types of detection systems to prevent false positives in your network.

IDSs are primarily focused on reporting events or network traffic that deviate from historical work activity or network traffic patterns. For this reporting to be effective, administrators should develop a baseline or history of typical network traffic. This baseline activity provides a stable, long-term perspective on network activity. An example might be a report generated when a higher-than-normal level of ICMP responses is

received in a specified time period. Such activity may indicate the beginning of an ICMP flood attack. The system may also report when a user who doesn't normally access the network using a VPN suddenly requests administrative access to the system. Figure 3.4 demonstrates an AD-IDS tracking and reporting excessive traffic in a network. The AD-IDS process frequently uses artificial intelligence or expert system technologies to learn about normal traffic for a network.

FIGURE 3.4 AD-IDS using expert system technology to evaluate risks



Whenever there is an attack, there is almost always something created that identifies it—an entry in the login report, an error in a log, and so forth. Those items represent intrusion signatures, and you can learn from them and instruct an IDS to watch for and prevent repeat performances of those items.

MD-IDS and AD-IDS are merging in most commercial systems. They provide the best opportunity to detect and thwart attacks and unauthorized access. Unlike a firewall, the IDS exists to detect and report unusual occurrences in a network, not block them.

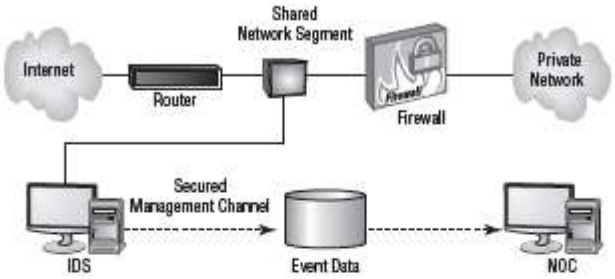
The next sections discuss network-based and host-based implementations of IDS and the capabilities they provide. I'll also introduce honeypots and incident response.

Working with a Network-Based IDS

A *network-based IDS (NIDS)* approach to IDS attaches the system to a point in the network where it can monitor and report on all network traffic. This can be in front of or behind the firewall, as shown in Figure 3.5.

The best solution to creating a secure network is to place the IDS in front of and behind the firewall. This double security provides as much defense as possible.

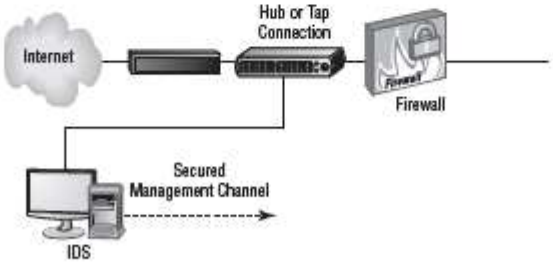
FIGURE 3.5 NIDS placement in a network determines what data will be analyzed.



Placing the NIDS in front of the firewall provides monitoring of all network traffic going into the network. This approach allows a huge amount of data to be processed, and it lets you see all the traffic coming into the network. Putting the NIDS behind the firewall only allows you to see the traffic that penetrates the firewall. Although this approach reduces the amount of data processed, it doesn't let you see all the attacks that might be developing.

The NIDS can be attached to a switch or a hub, or it can be attached to a tap. Many hubs and switches provide a monitoring port for troubleshooting and diagnostic purposes. This port may function in a manner similar to a tap. The advantage of the tap approach is that the IDS is the only device that will be using the tap. Figure 3.6 illustrates a connection to the network using a hub or tap.

FIGURE 3.6 A hub being used to attach the NIDS to the network



Port spanning, also known as *port mirroring*, copies the traffic from all ports to a single port and disallows bidirectional traffic on that port. Cisco's Switched Port Analyzer (SPAN) is one example of a port-spanning implementation.

In either case, the IDS monitors and evaluates all the traffic to which it has access.

Two basic types of responses can be formulated at the network level: passive and active. They're briefly explained in the following sections.

Real World Scenario

Working with Network Audit Files

You're the network administrator of a relatively busy network. Your company has gone through a couple of cutbacks, and your staffing is limited. You want to make sure that your network stays as secure as you can make it. What can you do to ease your workload?

You have three possibilities. There are two you should consider to protect your network: Either install an IDS or reduce the logging levels of your network audit files. An alternative is to install an audit log-collection system with filtering.

You might be able to reduce the amount of logged traffic in your audit files by changing the settings that determine what you audit. However, changing audit rules would prevent you from seeing what's happening on your network because most events wouldn't be logged.

Installing an IDS would allow you to establish rules that would provide a higher level of automation than you could achieve by reviewing audit files. Your best solution might be to convince your company to invest in an IDS. An IDS could send you an email or alert you when an event is detected.

Implementing a Passive Response

A *passive response* is the most common type of response to many intrusions. In general, passive responses are the easiest to develop and implement. The following list includes some passive response strategies:

Logging *Logging* involves recording that an event has occurred and under what circumstances it occurred. Logging functions should provide sufficient information about the nature of the attack to help administrators determine what has happened and to assist in evaluating the threat. This information can then be used to devise methods to counter the threat.

Notification *Notification* communicates event-related information to the appropriate personnel when an event has occurred. This includes relaying any relevant data about the event to help evaluate the situation. If the IDS is manned full time, messages can be displayed on the manager's console to indicate that the situation is occurring.

Shunning *Shunning* or ignoring an attack is a common response. This might be the case if your IDS notices an Internet Information Server (IIS) attack occurring on a system that's running another web-hosting service, such as Apache. The attack won't work because Apache

doesn't respond the same way that IIS does, so why pay attention to it? In a busy network, many different types of attacks can occur simultaneously. If you aren't worried about an attack succeeding, why waste energy or time investigating it or notifying someone about it? The IDS can make a note of it in a log and move on to other more pressing business.

Remember that passive responses are the most commonly implemented. They are the least costly and the easiest to put into practice.

Implementing an Active Response

An *active response* involves taking an action based on an attack or threat. The goal of an active response is to take the quickest action possible to reduce an event's potential impact. This type of response requires plans for how to deal with an event, clear policies, and intelligence in the IDS in order to be successful. An active response will include one of the reactions briefly described here:

Terminating Processes or Sessions If a flood attack is detected, the IDS can cause the subsystem, such as TCP, to force resets to all the sessions that are under way. Doing so frees up resources and allows TCP to continue to operate normally. Of course, all valid TCP sessions are closed and will need to be reestablished—but at least this will be possible, and it may have little effect on the end users. The IDS evaluates the events and determines the best way to handle them. Figure 3.7 illustrates TCP being directed to issue RST commands from the IDS to reset all open connections to TCP. This type of mechanism can also terminate user sessions or stop and restart any process that appears to be operating abnormally.

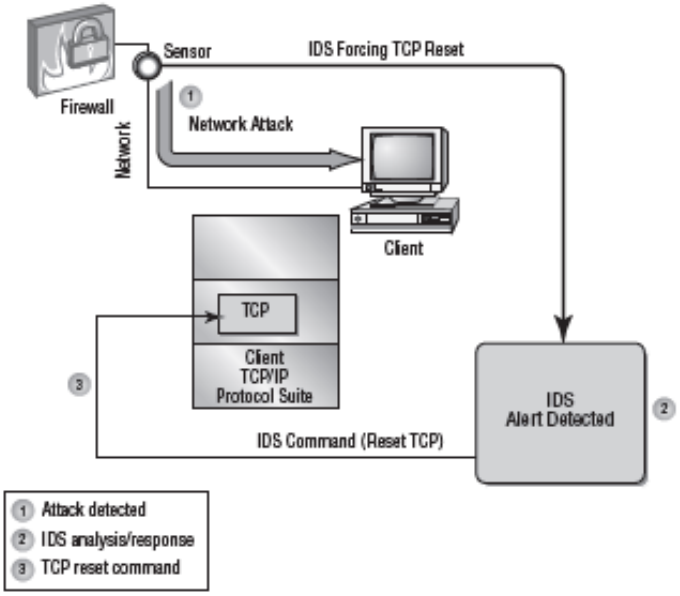
Network Configuration Changes If a certain IP address is found to be causing repeated attacks on the network, the IDS can instruct a border router or firewall to reject any requests or traffic from that address. This configuration change can remain in effect permanently or for a specified period. Figure 3.8 illustrates the IDS instructing the firewall to close port 80 for 60 seconds to terminate an IIS attack.

If the IDS determines that a particular socket or port is being attacked, it can instruct the firewall to block that port for a specified amount of time. Doing so effectively eliminates the attack but may also inadvertently cause a self-imposed DoS situation to occur by eliminating legitimate traffic. This is especially true for port 80 (HTTP or web) traffic.

Deception A *deception* active response fools the attacker into thinking the attack is succeeding while the system monitors the activity and potentially redirects the attacker to a system that is designed to be broken. This allows the operator or administrator to gather data about how the attack is unfolding and the techniques being used in the attack. This process is referred to as *sending them to the honeypot*, and it's described later in the section "Utilizing Honeypots." Figure 3.9 illustrates a honeypot where a deception has been successful.

The advantage of this type of response is that all activities are watched and recorded for analysis when the attack is completed. This is a difficult scenario to set up, and it's dangerous to allow a hacker to proceed into your network, even if you're monitoring the events.

FIGURE 3.7 IDS instructing TCP to reset all connections



This approach is frequently used when an active investigation is under way by law enforcement and they're gathering evidence to ensure a successful prosecution of the attacker. Deception allows you to gather documentation without risking live data.

Remember that active responses are the least commonly implemented. Those that are the most effective are the most costly and the hardest to put into practice, not to mention the trouble you can get into following a we-attack-those-who-attack-us strategy.

Working with a Host-Based IDS

A *host-based IDS (HIDS)* is designed to run as software on a host computer system. These systems typically run as a service or as a background process. HIDSs examine the machine logs, system events, and applications interactions; they normally don't monitor incoming network traffic to the host. HIDSs are popular on servers that use encrypted channels or channels to other servers.

FIGURE 3.8 IDS instructing the firewall to close port 80 for 60 seconds to thwart an IIS attack

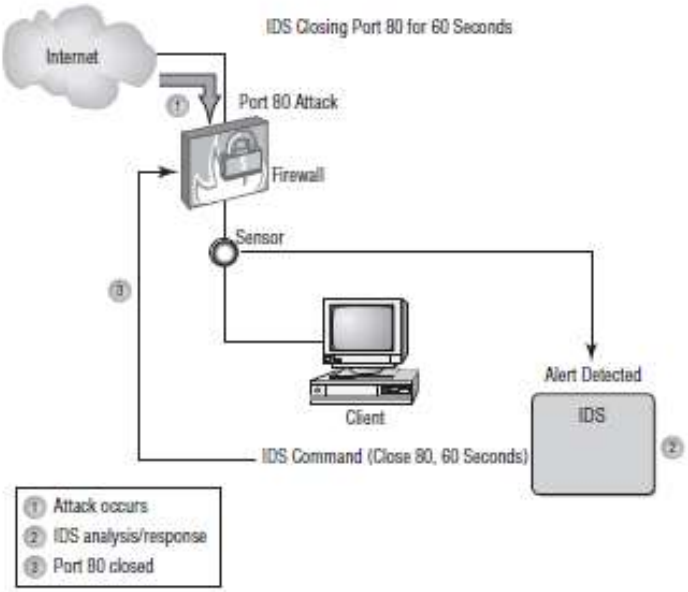


FIGURE 3.9 A network honeypot deceives an attacker and gathers intelligence.

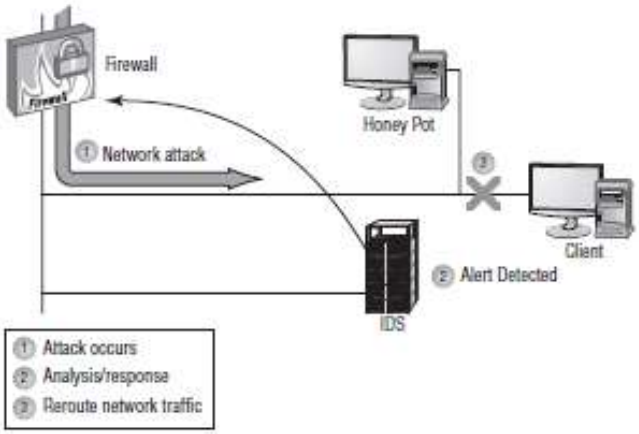
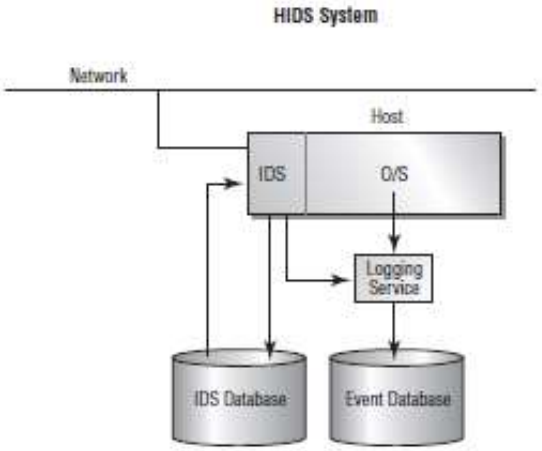


Figure 3.10 illustrates an HIDS installed on a server. Notice that the HIDS interacts with the logon audit and kernel audit files. The kernel audit files are used for process and application interfaces.

FIGURE 3.10 A host-based IDS interacting with the operating system



Two major problems with HIDS aren't easily overcome. The first problem involves a compromise of the system. If the system is compromised, the log files the IDS reports to may become corrupt or inaccurate. This may make fault determination difficult or the system unreliable. The second major problem with HIDS is that it must be deployed on each system that needs it. This can create a headache for administrative and support staff.

One of HIDS's major benefits is the potential to keep checksums on files. These checksums can be used to inform system administrators that files have been altered by an attack. Recovery is simplified because it's easier to determine where tampering has occurred.

Host-based IDSs typically respond in a passive manner to an incident. An active response would theoretically be similar to those provided by a network-based IDS.

Working with NIPS

As opposed to *Network Intrusion Detection Systems (NIDSs)*, Network Intrusion Prevention Systems (NIPSs) focus on *prevention*. These systems focus on signature matches and then take a course of action. For example, if it appears as if an attack might be under way, packets can be dropped, ignored, and so forth. In order to be able to do this, the NIPS must be able to *detect* the attack occurring, and thus it can be argued that NIPS is a subset of NIDS.

The line continues to blur between technologies. For example, NIST now refers to its releases as IDPS. While it is important to stay current on the terminology in the real world, know that the exam is frozen in time and you should be familiar with the older terminology for the questions you will face on it.

Log Files in Linux

There are a number of logs to check for entries that might indicate an intrusion. The primary ones you should examine are listed here:

/var/log/faillog Open a shell prompt and use the `faillog` utility to view a list of users' failed authentication attempts.

/var/log/lastlog Open a shell prompt and use the `lastlog` utility to view a list of all users and when they last logged in.

/var/log/messages Use grep, or a derivative thereof, to find login-related entries in this file.

/var/log/wtmp Open a shell prompt and use the `last` command to view a list of users who have authenticated to the system.

Utilizing Honeypots

A *honeypot* is a computer that has been designated as a target for computer attacks. The best way to visualize a honeypot is to think of Winnie the Pooh and the multiple times the character has become stuck while trying to get the honey out of the jugs it is stored in. By getting stuck, he has incapacitated himself and become an easy target for anyone trying to find him.

Two of the most popular honeypots for Linux are honeyd (`http://honeyd.org`) and Tiny Honeypot (thp) (`http://freshmeat.net/projects/thp/`).

The purpose of a honeypot is to allow itself to succumb to an attack. During the process of "dying," the system can be used to gain information about how the attack developed and what methods were used to institute the attack. The benefit of a honeypot system is that it draws attackers away from a higher-value system or allows administrators to gain intelligence about an attack strategy. See Figure 3.9 for a diagram of a honeypot implementation.

Honeypots aren't normally secured or locked down. If they come straight out of the box with an operating system and applications software, they may be configured as is. Elaborate honeypot systems can contain information and software that might entice an attacker to

probe deeper and take over the system. If not configured properly, a honeypot system can be used to launch attacks against other systems.

There are several initiatives in the area of honeypot technology. One of the more interesting involves the Honeynet Project, which created a synthetic network that can be run on a single computer system and is attached to a network using a normal network interface card (NIC). The system looks like an entire corporate network, complete with applications and data, all of which are fake. As part of the Honeynet Project, the network was routinely scanned, worms were inserted, and attempts were made to contact other systems to infest them—all over the course of a three-day period. At the end of day three, the system had been infected by no fewer than three worms. This infestation happened without any advertising by the Honeynet Project.

Additional information is available on the Honeynet Project at `http://www.honeynet.org/`.

Before you even consider implementing a honeypot or a honeynet-type project, you need to understand the concepts of *enticement* and *entrapment*:

Enticement *Enticement* is the process of luring someone into your plan or trap. You might accomplish this by advertising that you have free software, or you might brag that no one can break into your machine. If you invite someone to try, you're enticing them to do something that you want them to do.

Entrapment *Entrapment* is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution.

While enticement is legally acceptable, entrapment isn't. Your legal liabilities are probably small in either case, but you should seek legal advice before you implement a honeypot on your network. You may also want to contact law enforcement or the prosecutor's office if you want to pursue legal action against attackers.

Some security experts use the term *tar pit* in place of honeypot. The two terms are interchangeable.

Understanding Protocol Analyzers

The terms *protocol analyzing* and *packet sniffing* are interchangeable. They refer to the process of monitoring the data that is transmitted across a network. The software that performs the operation is called either an *analyzer* or a *sniffer*, as mentioned in the "Network Monitors" section at the beginning of this chapter. Sniffers are readily available on the Internet. These

tools were initially intended for legitimate network-monitoring processes, but they can also be used to gather data for illegal purposes.

IM traffic, for example, uses the Internet and is susceptible to packet-sniffing activities. Any information contained in an IM session is potentially vulnerable to interception. Make sure users understand that sensitive information should not be sent using this method.

One of the best-known tools for analyzing network traffic in real time is Snort (`http://www.snort.org`). Exercise 3.1 walks through the installation of this tool.

EXERCISE 3.1

Install Snort in Linux

The de facto standard for intrusion detection in Linux is Snort. To install the package on a SuSE server, follow these steps:

1. Log in as root and start YaST.
2. Choose Software and then Install And Remove Software. Search for **snort**.
3. Check the box when the package appears.
4. Click Accept. If any dependency messages appear, click Continue to add them as well.
5. Swap CDs as prompted and exit YaST upon completion.

To use the Snort utility, open a terminal session and type **snort**. This generates an error message that lists all the options that you can use with the utility.

Securing Workstations and Servers

Workstations are particularly vulnerable in a network. Most modern workstations, regardless of their operating systems, communicate using services such as file sharing, network services, and applications programs. Many of these programs have the ability to connect to other workstations or servers.

Because a network generally consists of a minimal number of servers and a large number of workstations, it's often easier for a hacker to find an unsecure workstation and enter there first. Once the hacker has gained access to the workstation, it becomes easier to access the network since they're now inside the firewall.

These connections are potentially vulnerable to interception and exploitation. The process of making a workstation or a server more secure is called *platform hardening*. The process of

hardening the operating system is referred to as *OS hardening*. (OS hardening is part of platform hardening, but it deals only with the operating system.) Platform hardening procedures can be categorized into three basic areas:

- Remove unused software, services, and processes from the workstations (for example, remove the server service from a workstation). These services and processes may create opportunities for exploitation.
- Ensure that all services and applications are up-to-date (including available service and security packs) and configured in the most secure manner allowed. This may include assigning passwords, limiting access, and restricting capabilities.
- Minimize information dissemination about the operating system, services, and capabilities of the system. Many attacks can be targeted at specific platforms once the platform has been identified. Many operating systems use default account names for administrative access. If at all possible, these should be changed. During a new installation of Windows 7 or Windows Vista, the first user created is automatically added to the Administrators group. Windows then goes one step further and automatically disables the actual administrator account once another account belonging to the Administrators group has been created. Earlier versions of Windows did not do this and the account was enabled. In Linux, the root user account is automatically created during installation as well.

One way to prevent users from making changes in Microsoft operating systems is to lock their configuration settings. This is possible with Windows clients through the use of group policies.

Most modern server products also offer workstation functionality. In fact, many servers are virtually indistinguishable from workstations. Linux functions as both a workstation and a server in most cases.

Most successful attacks against a server will also work against a workstation, and vice versa. Additionally, servers run dedicated applications, such as SQL Server or a full-function web server.

An early version of Internet Information Services (IIS) included a default mail system as a part of its installation. This mail system was enabled unless specifically disabled. It suffered from most of the vulnerabilities to virus and worm infections discussed in Chapter 4. Make sure your system runs only the services, protocols, and processes you need. Turn off or disable things you don't need.

When you're looking for ways to harden a server, never underestimate the obvious. You should always apply all patches and fixes that have been released for the operating system. Additionally, you should make certain you aren't running any services that aren't needed on the machine.

Real World Scenario

Users Installing Unauthorized Software

Members of your Information Systems (IS) department are upset about the amount of unauthorized software that is being installed on many of the Windows clients on your network. They come to you for advice on how to minimize the impact of this software. What do you tell them?

All newer Windows clients allow permissions to be established to prevent software installation. You should evaluate the capabilities of the settings in the workstations for security. This process is referred to as *locking down* a desktop. You can lock down most desktops to prevent the installation of software. Yet although this may sound like a great solution, remember that doing so may also prevent users from automatically upgrading software and may create additional work for the IS department. You'll need to evaluate both issues to determine the best approach to take and then make your recommendation to the IS department.

Real World Scenario

Finding Ways to Harden Your Servers

Armed with a list of the different types of servers on your network, look for ways in which they can be hardened by answering the following questions:

1. Are there services running on them that aren't needed?
2. Have the latest patches and fixes been applied?
3. Are there known issues with this operating system?
4. Are there known issues with the services or applications that are running?

One of the first tasks you should do is to go to a search engine and enter the word *hardening* along with the exact operating system you're running.

Securing Internet Connections

The Internet is perhaps the area of largest growth for networks. The technology started as a research project funded by the Department of Defense and has grown at an enormous rate. Within a few years, virtually every computer in the world is expected to be connected

to the Internet. This situation creates a security nightmare and is one of the primary reasons the demand for professionals trained in information and computer security is expected to grow exponentially.

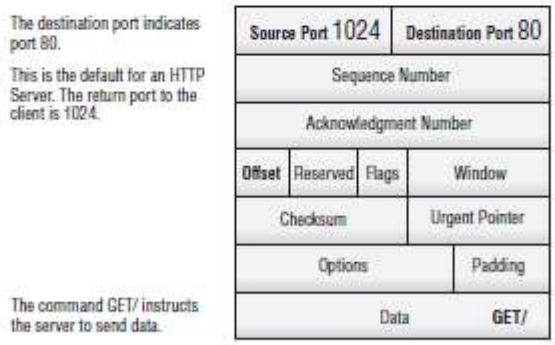
The following sections describe ports and sockets and then some of the more common protocols, including email, web, and FTP, that you should be familiar with for the exam.

Working with Ports and Sockets

As we've already discussed, the primary method of connection between systems using the Internet is TCP/IP. This protocol establishes connections and circuits using a combination of the IP address and a port. A *port* is an interface that is used to connect to a device. *Sockets* are a combination of the IP address and the port. For example, if you attempt to connect to a remote system with the IP address 192.168.0.100, which is running a website, you'll use port 80 by default. The combination of these two elements gives you a socket. The full address and socket description would then be 192.168.0.100:80.

IP is used to route the information from one host to another through a network. The four layers of TCP/IP encapsulate the information into a valid IP packet that is then transmitted across the network. Figure 3.11 illustrates the key components of a TCP packet requesting the home page of a website. The data will be returned from the website to port 1024 on the originating host.

FIGURE 3.11 A TCP packet requesting a web page from a web server



The source port is the port that is addressed on the destination. The destination port is the port to which the data is sent. In the case of a web application, the data for both port addresses would contain 80. A number of the fields in this packet are used by TCP for verification and integrity, and you need not be concerned with them at this time.

However, the data field contains the value `Get/`. This value requests the home or starting page from the web server. In essence, this command or process requested the home page of

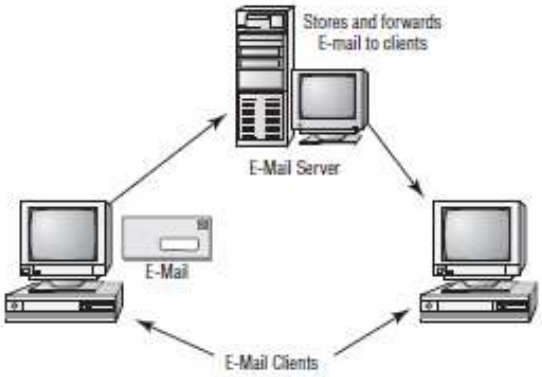
the site 192.168.0.100 port 80. The data is formed into another data packet that is passed down to IP and sent back to the originating system on port 1024.

The connections to most services using TCP/IP are based on this port model. Many of the ports are well documented, and the protocols to communicate with them are well known. If a vendor has a technological weakness or implements security poorly, the vulnerability will become known and exploited in a short time.

Working with Email

Email is one of the most popular applications in use on the Internet. Several good email servers and clients are available. Figure 3.12 demonstrates the process of transferring an email message.

FIGURE 3.12 Email connections between clients and a server



The most common email systems use the following protocols, which use TCP for session establishment:

Simple Mail Transport Protocol *Simple Mail Transport Protocol (SMTP)* is a mail delivery protocol that is used to send email between an email client and an email server as well as between email servers. Messages are moved from client to server to client via the Internet. Each email message can take a different path from the client to the server. In the case of Figure 3.12, the clients are on two different email servers; they could both be on the same server, and the process would appear transparent to the user. SMTP uses port 25 and TCP for connections.

Post Office Protocol *Post Office Protocol (POP)* is a newer protocol that relies on SMTP for message transfer to receive email. POP provides a message store that can be used to store and forward messages. If a server isn't operating, the originating server can store a message

and try to resend it later. POP3, the newest version of POP, allows messages to be transferred from the waiting post office to the email client. The current POP standard uses port 109 for POP2 and 110 for POP3. POP uses TCP for connections.

Internet Message Access Protocol *Internet Message Access Protocol (IMAP)* is the newest player in the email field, and it's rapidly becoming the most popular. Like POP, IMAP has a store-and-forward capability. However, it has much more functionality. IMAP allows messages to be stored on an email server instead of being downloaded to the client. It also allows messages to be downloaded based on search criteria. Many IMAP implementations also allow connections using web browsers. The current version of IMAP (IMAP 4) uses port 143 and TCP for connections.

S/MIME and *PGP* are two of the more popular methods of providing security for emails. We discuss these in Chapter 8.

Working with the Web

When two hosts communicate across the Web, data is returned from the host using *Hypertext Markup Language (HTML)*. HTML is nothing more than a coding scheme to allow text and pictures to be presented in a specific way in a web browser. HTML can be created any number of ways, including via manual coding and in graphical design programs. HTML files are read, interpreted by your browser, and displayed on your system. If you want to see what HTML looks like, you can set your browser to view source code—you'll see things similar to word-processor coding for virtually every characteristic of the web page you're viewing.

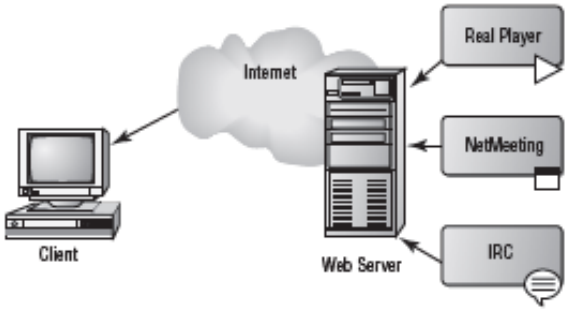
Websites are collections of these pages, which are called into your browser when you click a link or scroll through the pages. Most developers want more than the ability to display pages and pages of colored text on your computer. To make creative and sophisticated websites possible, web browsers have become more complicated, as have web servers. Current browsers include audio, visuals, animations, live chats, and almost any other feature you can imagine.

Figure 3.13 illustrates some of the content that can be delivered over the Internet via a web server.

This ability to deliver content over the Web is accomplished in one of several ways. The most common approach involves installing applications that talk through the server to your browser. The applications require additional ports to be opened through your firewall and routers. Unfortunately, doing so inherently creates security vulnerabilities.

Each port you leave open in your network increases your vulnerability. For instance, if you open the ports necessary to use the popular program NetMeeting, you're exposing your users to additional opportunities for attack. NetMeeting, like many other programs, has had a number of security vulnerabilities in the past, and it will probably have more in the future.

FIGURE 3.13 A web server providing streaming video, animation, and HTML data to a client



Each of the popular web services is now offered in conjunction with web-enabled programs such as Flash and Java. These services use either a socket to communicate or a program that responds to commands through the browser. If your browser can be controlled by an application, your system is at great risk of being coerced into giving attackers information you don't want them to have. Servers are also vulnerable to this issue because they must process requests from browsers for information or data. A little research into the vulnerabilities of a proposed new service may save you a lot of time later should you become the target of an attack.

While HTML remains popular, *Extensible Markup Language (XML)* has also been adopted by many. Although it's not a replacement for HTML, XML offers many capabilities that HTML does not. These include the ability to describe the information (and not just display it). By being able to describe the data, it can display it across several platforms, systems, and so forth.

The best solution for many of the vulnerabilities that exist on the Web is to implement secure web connections—the topic of our next section.

Secure Web Connections

There are two common ways to provide secure connections between a web client and a web server:

Secure Sockets Layer and Transport Layer Security *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)* are two common protocols used to convey information between a web client and a server. The SSL protocol uses an encryption scheme between the two systems. The client initiates the session, the server responds, indicating that encryption is needed, and then they negotiate an appropriate encryption scheme. TLS is a newer protocol that merges SSL with other protocols to provide encryption. TLS supports SSL connections for compatibility, but it also allows other encryption protocols, such as Triple DES, to be used. SSL/TLS uses port 443 and TCP for connections.

HTTP/S *HTTP Secure (HTTP/S)* is a protocol that is used for secure connections between two systems that use the Web. It protects the connection, and all traffic between the two systems is encrypted. HTTP/S uses SSL or TLS for connection security, and it uses port 443 and TCP for connections.

Don't confuse Secure HTTP (S-HTTP) with HTTP/S. S-HTTP is a different protocol that lets systems negotiate an encryption connection between each other. S-HTTP can provide some of the capabilities of HTTP/S, but it isn't as secure and is rarely used in practice, but it makes for an excellent exam question.

Vulnerabilities of Web Add-ins

The growth of the Web and demands from users for more features have spurred the creation of a new set of vulnerabilities that must be evaluated and managed. Increasingly, web browsers and other web-enabled technologies allow servers to send instructions to the client to provide multimedia and other capabilities. This is creating a problem for security professionals because these protocols offer potential weaknesses.

The following sections discuss the more common web-based applications, such as JavaScript and applets, and the vulnerabilities you should be aware of. These vulnerabilities can include malicious code, viruses, and exploitations.

ActiveX

ActiveX is a technology that was implemented by Microsoft to customize controls, icons, and other features, which increases the usability of web-enabled systems. ActiveX runs on the client. It uses a method called *Authenticode* for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server.

ActiveX components are downloaded to the client hard disk, potentially allowing additional security breaches. Web browsers can be configured so that they require confirmation to accept an ActiveX control. However, many users don't understand these confirmation messages when they appear, and they automatically accept the components. Automatically accepting an ActiveX component or control creates the opportunity for security breaches on a client system when the control is used because an ActiveX control contains programming instructions that can contain malicious code or create vulnerabilities in a system.

It's highly recommended that browsers be configured so that they do not allow ActiveX to run without prompting the user because of the potential security hole that could be opened.

Buffer Overflows

Buffer overflows occur when an application receives more data than it's programmed to accept. This situation can cause an application to terminate or to write data beyond the end

of the allocated space. Termination may leave the system sending the data with temporary access to privileged levels in the attacked system, while overwriting can cause important data to be lost. This exploitation is usually a result of a programming error in the development of the software.

Buffer overflows, while a less-common source of exploitation than in the past, are still quite common and far from a small problem.

Common Gateway Interface

Common Gateway Interface (CGI) is an older form of scripting that was used extensively in early web systems. CGI scripts were used to capture data from a user using simple forms. They aren't widely used in new systems and are being replaced by Java, ActiveX, and other technologies.

CGI scripts run on the web server and interact with the client browser. CGI is often frowned upon in new applications because of its security issues, but it's still widely used in older systems. Vulnerabilities in CGI are the result of its inherent ability to do what it is told. If a CGI script is written to wreak havoc (or carries extra code added to it by a miscreant) and it is executed, your systems will suffer. The best protection against any weaknesses is to not run applications written in CGI but rather to opt for those written in the newer languages where possible.

Cookies

Cookies are text files that a browser maintains on the user's hard disk in order to provide a persistent, customized web experience for each visit. A cookie typically contains information about the user. For example, a cookie can contain a client's history to improve customer service. If a bookstore wants to know your buying habits and what types of books you last viewed at its site, it can load this information into a cookie on your system. The next time you return to that store, the server can read your cookie and customize what it presents to you. Cookies can also be used to time-stamp a user to limit access. A financial institution may send your browser a cookie once you've authenticated. The server can read the cookie to determine when a session is expired.

Obviously, cookies are considered a risk because they have the potential to contain your personal information, which could get into the wrong hands, and are highly treasured by advertisers today. A new breed of cookie known as *evercookie* writes data to multiple locations to make it next to impossible to ever remove it completely (see `http://samy.pl/evercookie/`).

If security is your utmost concern, the best protection is to not allow cookies to be accepted. Almost every browser offers the option of enabling or disabling cookies. If you enable them, you can usually choose whether to accept/reject all or only those from an originating server.

Cross-Site Scripting

Using a client-side scripting language, it is possible for a ne'er-do-well to trick a user into visiting their site and have code then execute locally. When this is done, it is known as *cross-site scripting (XSS)*. As an example, UserA may get a message telling him that he needs to make

changes to his XYZ account, but the link in the message is not really to the XYZ site (a phishing ploy). When he clicks the link, a JavaScript routine begins to run on his machine. Since the script is running on UserA's system, it has his permissions and can begin doing such things as running malevolent routines to send/delete/alter data.

The best protection against cross-site scripting is to disable the running of scripts.

Input Validation

Anytime a user must supply values in a session, the data entered should be validated. Many vendors, however, have fallen prey to *input validation* vulnerabilities within their code. In some instances, empty values have been accepted, while others have allowed privilege escalation if certain backdoor passwords were used.

The best protection against input-validation vulnerabilities is for developers to follow best practices and always validate all values entered. As an administrator, when you learn of an input-validation vulnerability with any application on your system, you should immediately stop using it until a patch has been released and installed.

Java Applets

A *Java applet* is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they're becoming one of the most popular tools used for website development.

Java-enabled applications can accept programmed instructions (Java scripts) from a server and control certain aspects of the client environment. Java requires you to download a virtual machine in order to run the Java applications or applets. Java scripts run on the client.

The applets run in a restricted area of memory called the *sandbox*. The sandbox limits the applet's access to user areas and system resources. An applet that runs in the sandbox is considered *safe*, meaning it won't attempt to gain access to sensitive system areas. Errors in the Java virtual machine that runs in the applications may allow some applets to run outside the sandbox. When this occurs, the applet is unsafe and may perform malicious operations. Attackers on client systems have exploited this weakness. From a user's standpoint, the best defense is to make certain you run only applets from reputable sites you're familiar with. From an administrator's standpoint, you should make certain programmers adhere to programming guidelines when creating the applets.

JavaScript

JavaScript is a programming language that allows access to system resources of the system running a script. A JavaScript script is a self-contained program that can be run as an executable file in many environments. These scripts can interface with all aspects of an operating system, just as programming languages such as the C language can. This means that JavaScript scripts, when executed, can potentially damage systems or be used to send information to unauthorized persons. JavaScript scripts can be downloaded from a website and executed.

Popups

While not technically an add-in, *popups* (also known as pop-ups) are both frustrating and chancy. Whenever a user visits a website and another instance (either another tab or

another browser window) is opened in the foreground, it is called a popup; if it opens in the background, it is called a popunder. Both popups and popunders open pages or sites that the user did not specifically request and may only display ads, but they might bring up undesirable applets.

Popup blockers are used to prevent both popups and popunders from appearing. While older browsers did not incorporate an option to block popups, most newer browsers now have that capability built in.

Signed Applets

Signed applets are similar to Java applets, with two key differences: A signed applet doesn't run in the Java sandbox, and it has higher system access capabilities. Signed applets aren't usually downloaded from the Internet; this type of applet is typically provided by in-house or custom-programming efforts. These applets can also include a digital signature to verify authenticity. If the applet is verified as authentic, it will be installed. Users should never download a signed applet unless they're sure the provider is trusted. A signed applet from an untrustworthy provider has the same security risks as an unsigned applet.

A vulnerability reveals itself when an applet is always assumed to be safe because it is signed. Being signed, it may have the ability to do things outside the realm of normal applets, such as execute programs. A disgruntled programmer can create a malicious signed applet and wreak havoc until stopped.

Most web browsers have settings that can be used to control Java access. This allows clients to control resource access using Java applets or scripts.

SMTP Relay

SMTP relay is a feature designed into many email servers that allows them to forward email to other email servers. Initially, the SMTP relay function was intended to help bridge traffic between systems. This capability allows email connections between systems across the Internet to be made easily.

Unfortunately, this feature has been used to generate a great deal of spam on the Internet. An email system that allows this type of forwarding to occur is referred to as an *open relay*. Unscrupulous individuals can use open relays to send advertisements and other messages through open relay servers, and they can post your mail server on lists for others to use (which could lead to your server being blacklisted). SMTP relaying should be disabled on your network unless it's limited to the email servers in your domain.

Working with File Transfer Protocol

File Transfer Protocol (FTP) was the most common protocol used to transfer files between systems on the Internet for many years, and it's available on most major server environments.

Real World Scenario

SMTP Relaying in Action

You've just received a call from a client indicating that their email server is acting peculiarly. When you arrive at the site, you notice that there are more than 20,000 emails in the outbound mail folder and that the system has no disk space available. When you shut down the email software, you delete these files and restart the email server. You see that the outbound mail folder begins to fill up again. What problem could this server be encountering?

E-marketers may be using the server as a relay. This hijacking will continue until you disable the SMTP relay capabilities in the server. Many older systems don't allow SMTP relaying to be turned off; such servers must be upgraded or replaced to prevent this from continuing.

The Internet has replaced many of the functions FTP served in the past. FTP is still commonly used, but it's becoming less popular as other methods of file downloading are made available. Most popular browsers allow an FTP site to be accessed as a website, and HTTP supports file transfer capabilities. A browser provides a graphical interface that users can use without having to be exposed to the command structure that FTP uses by default.

The following sections discuss FTP, its vulnerabilities, and ways to secure it.

Blind/Anonymous FTP

Early FTP servers didn't offer formal security—security was based on the honor system. In most cases, the honor system was used strictly for downloading files from an FTP server to a client; a client couldn't upload files without using a different logon ID. In some cases, the opposite situation existed, and a client could "blindly" upload files for others but could not download—or even see—any files.

Most logons to an FTP site used the anonymous logon; by convention, the logon ID was anonymous, and the password was the user's email address. This honor system is still used in systems that want to allow public access to files, and it simplifies administration because only one account is used.

The cost of this implementation, however, is the risk that is taken on. In this situation, the only security offered is what is configured by the operating system.

Secure FTP

Secure FTP (S/FTP or SFTP) is accomplished using a protocol called *Secure Shell (SSH)*—a type of tunneling protocol that allows access to remote systems in a secure manner. As discussed earlier, SSH allows connections to be secured by encrypting the session between the client and the server. SSH is available for Unix and other systems that provide capabilities similar to FTP.

Sharing Files

File sharing is accomplished by storing files at an assigned location on the server or workstation. When files are stored on a workstation, the connection is referred to as a *peer-to-peer connection*. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation.

In an FTP connection, you can upload a file from a client using the PUT command. You download using the GET command. Most modern servers and applications allow an application program to access shared files at the record level. This type of sharing allows multiuser applications, such as databases, to function. Web browsers typically accept files from a web server by downloading them from the server. These downloaded files are then processed through the browser and displayed to the user.

FTP's Vulnerability

FTP has a major flaw: The user ID and password aren't encrypted and are subject to packet capture. This creates a major security breach—especially if you're connecting to an FTP server across the Internet. There is also a problem if you're allowing the use of the anonymous version of FTP: *Trivial File Transfer Protocol (TFTP)*. TFTP is a UDP-based service and has no username or password and can be used to transfer files in unattended mode.

Real World Scenario

Remote File Transfers

Your organization has a large number of remote users who transfer files to your system across the Internet. These file transfers are an essential part of your business, and they must be allowed to continue. You want to provide additional security to your users so that information won't be compromised. How might you accomplish this?

You could implement SSH or other secure protocols for FTP file transfers. Doing so would allow information to be sent across the Internet in a secure manner. You may also be able to use TLS, SSL, or another secure format.

Understanding Network Protocols

Your network may have network protocols running in addition to TCP/IP, and each of these protocols may be vulnerable to outside attack. Some protocols (such as NetBEUI, DLC, and other more primitive protocols) aren't routable and, therefore, aren't subject to attack. Of course, there is a great big "unless": If your router or firewall is configured to pass them, some of these protocols can be imbedded in TCP/IP and may be passed to other systems.

The major protocols used by TCP/IP for maintenance and other activities include those discussed in the following list:

Simple Network Management Protocol TCP/IP uses *Simple Network Management Protocol (SNMP)* to manage and monitor devices in a network. Many copiers, fax machines, and other smart office machines use SNMP for maintenance functions. This protocol travels through routers quite well and can be vulnerable to attack. Although such an attack might not be dangerous, think about what could happen if your printer suddenly went online and started spewing paper all over the floor.

SNMP was upgraded as a standard to SNMPv2, which provides security and improved remote monitoring. SNMP is currently undergoing a revision; although a new standard (SNMPv3) is out, most systems still use SNMPv2.

Internet Control Message Protocol TCP/IP uses *Internet Control Message Protocol (ICMP)* to report errors and reply to requests from programs such as Ping and Traceroute. ICMP is one of the favorite protocols used for DoS attacks. Many businesses have disabled ICMP through the router to prevent these types of situations from occurring.

Real World Scenario

Disabling ICMP to Deal with Smurf Attacks

Your organization has been repeatedly hit by smurf attacks (an attack that uses IP spoofing and broadcasting to send a ping to a group of hosts in a network). These attacks have caused a great deal of disruption, and they must be stopped. What could you suggest to minimize these attacks?

You should recommend disabling ICMP traffic at the point where your network connects to the Internet. You can do this by disabling the protocol on your router and blocking this traffic in firewall systems. Doing so won't completely eliminate the problem, but it will greatly reduce the likelihood of a successful attack occurring using ICMP. This step will also prevent people from gaining information about your network because any programs (such as Ping) that request information from your network systems will no longer function.

Internet Group Management Protocol TCP/IP uses *Internet Group Management Protocol (IGMP)* to manage group or multicasting sessions. It can be used to address multiple recipients of a data packet: The sender initiates broadcast traffic, and any client who has broadcasting enabled receives it. (*Broadcasts* are messages sent from a single system to the entire network—the systems could be inside your network or throughout the world.) This process, called *multicasting*, can consume huge amounts of bandwidth in a network and possibly create a DoS situation. Most network administrators disable the reception of broadcast and multicast traffic from outside their local network.

A *unicast* is IGMP traffic that is oriented at a single system. TCP/IP primarily uses a unicast method of communication: A message is sent from a single system to another single system.

Every one of these major protocols used by TCP/IP presents a potential problem for security administrators. Make sure you use what you need and disable what you don't.

Summary

In this chapter, I covered ports and sockets. Sockets are the primary method used to communicate with services and applications. Sockets are changeable for special configurations and additional security.

Network monitors are primarily troubleshooting tools, and they can be used to eavesdrop on networks. Intrusion detection systems take an active role and can control traffic and systems. IDSs use extensive rule-based procedures to check audit files and network traffic, and they can make decisions based on those rules. In conjunction with a firewall, an IDS can offer high levels of security.

Exam Essentials

Familiarize yourself with the technologies used by TCP/IP and the Internet. IP addresses and port numbers are combined to create an interface called a socket. Most TCP and UDP protocols communicate using this socket as the primary interface mechanism. Clients and servers communicate using ports. Ports can be changed to enhance security. Web services use HTML and other technologies to allow rich and animated websites. These technologies potentially create security problems because they may have individual vulnerabilities. Verify the problems that exist from a security perspective before enabling these technologies on your systems.

Be able to describe the primary methods used for network monitoring. The primary methods used for network monitoring are sniffers and IDSs. Sniffers are passive and can provide real-time displays of network traffic. They're intended to be used primarily for troubleshooting purposes, but they're one of the tools used by attackers to determine what protocols and systems you're running. IDSs are active devices that operate to alert administrators of attacks and unusual events. This is accomplished by automatically reviewing log files and system traffic and by applying rules that dictate how to react to events. An IDS, when used in conjunction with firewalls, can provide excellent security for a network.

Be able to identify and describe the two types of intrusion detection systems in use. The two types of IDSs in use are host-based (HIDS) and network-based (NIDS). Host-based IDS works strictly on the system on which it's installed. Network-based IDS monitors the entire network.

Be able to identify and explain the terms and functions in an IDS environment. These terms include *activity*, *administrator*, *alert*, *analyzer*, *data source*, *event*, *manager*, *notification*, *operator*, and *sensor*. For simplicity's sake, some of these systems are combined in IDSs, but they're all functions that must be performed to be effective.

Know the difference between an active response and a passive response. An active response allows an IDS to manage resources in the network if an incident occurs. Passive responses involve notification and reporting of attacks or suspicious activities.

Be able to explain the purpose of a honeypot. A honeypot is a system that is intended to be used to gather information or designed to be broken. Honeypot systems are used to gather evidence in an investigation and to study attack strategies.

Review Questions

1. In order for network monitoring to work properly, you need a PC and a network card running in what mode?
   - **A.** Launch
   - **B.** Exposed
   - **C.** Promiscuous
   - **D.** Sweep
2. Which Linux utility can show if there is more than one set of documentation on the system for a command you are trying to find information on?
   - **A.** `Lookaround`
   - **B.** `Howmany`
   - **C.** `Whereall`
   - **D.** `Whatis`
3. In intrusion detection system parlance, which account is responsible for setting the security policy for an organization?
   - **A.** Supervisor
   - **B.** Administrator
   - **C.** Root
   - **D.** Director
4. Which of the following IDS types looks for things outside of the ordinary?
   - **A.** Incongruity-based
   - **B.** Variance-based
   - **C.** Anomaly-based
   - **D.** Difference-based
5. Which of the following copies the traffic from all ports to a single port and disallows bidirectional traffic on that port?
   - **A.** Port spanning
   - **B.** Socket blending
   - **C.** Straddling
   - **D.** Amalgamation
6. Which of the following implies ignoring an attack and is a common response?
   - **A.** Eschewing
   - **B.** Spurning
   - **C.** Shirking
   - **D.** Shunning

7. Which IDS system uses algorithms to analyze the traffic passing through the network?
   A. Arithmetical
   B. Algebraic
   C. Statistical
   D. Heuristic
8. Which of the following utilities can be used in Linux to view a list of users' failed authentication attempts?
   A. `badlog`
   B. `faillog`
   C. `wronglog`
   D. `killlog`
9. Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead?
   A. Enticement
   B. Entrapment
   C. Deceit
   D. Sting
10. The IDS console is known as what?
    A. Manager
    B. Window
    C. Dashboard
    D. Screen
11. Sockets are a combination of the IP address and which of the following?
    A. Port
    B. MAC address
    C. NIC setting
    D. NetBIOS ID
12. Which type of active response fools the attacker into thinking the attack is succeeding while the system monitors the activity and potentially redirects the attacker to a system that is designed to be broken?
    A. Pretexting
    B. Shamming
    C. Deception
    D. Scamming

13. Which device monitors network traffic in a passive manner?
    A. Sniffer
    B. IDS
    C. Firewall
    D. Web browser

14. Security has become the utmost priority at your organization. You're no longer content to act reactively to incidents when they occur—you want to start acting more proactively. Which system performs active network monitoring and analysis and can take proactive steps to protect a network?
    A. IDS
    B. Sniffer
    C. Router
    D. Switch

15. Which of the following can be used to monitor a network for unauthorized activity? (Choose two.)
    A. Network sniffer
    B. NIDS
    C. HIDS
    D. VPN

16. You're the administrator for Acme Widgets. After attending a conference on buzzwords for management, your boss informs you that an IDS should be up and running on the network by the end of the week. Which of the following systems should be installed on a host to provide IDS capabilities?
    A. Network sniffer
    B. NIDS
    C. HIDS
    D. VPN

17. Which of the following is an active response in an IDS?
    A. Sending an alert to a console
    B. Shunning
    C. Reconfiguring a router to block an IP address
    D. Making an entry in the security audit file

18. A junior administrator bursts into your office with a report in his hand. He claims that he has found documentation proving that an intruder has been entering the network on a regular basis. Which of the following implementations of IDS detects intrusions based on previously established rules that are in place on your network?
    A. MD-IDS
    B. AD-IDS
    C. HIDS
    D. NIDS

19. Which IDS function evaluates data collected from sensors?
    A. Operator
    B. Manager
    C. Alert
    D. Analyzer

20. What is a system that is intended or designed to be broken into by an attacker called?
    A. Honeypot
    B. Honeybucket
    C. Decoy
    D. Spoofing system

Answers to Review Questions

1. C. In order for network monitoring to work properly, you need a PC and a network card running in promiscuous mode.
2. D. In Linux, the `whatis` utility can show if there is more than one set of documentation on the system for a command you are trying to find information on.
3. B. The administrator is the person/account responsible for setting the security policy for an organization.
4. C. An anomaly-detection IDS (AD-IDS) looks for anomalies, meaning it looks for things outside of the ordinary.
5. A. Port spanning (also known as port mirroring) copies the traffic from all ports to a single port and disallows bidirectional traffic on that port.
6. D. Shunning, or ignoring an attack, is a common response.
7. D. A heuristic system uses algorithms to analyze the traffic passing through the network.
8. B. Use the `faillog` utility in Linux to view a list of users' failed authentication attempts.
9. B. Entrapment is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead.
10. A. The IDS console is known as the manager.
11. A. Sockets are a combination of the IP address and the port.
12. C. A deception active response fools the attacker into thinking the attack is succeeding while the system monitors the activity and potentially redirects the attacker to a system that is designed to be broken.
13. A. Sniffers monitor network traffic and display traffic in real time. Sniffers, also called network monitors, were originally designed for network maintenance and troubleshooting.
14. A. An IDS is used to protect and report network abnormalities to a network administrator or system. It works with audit files and rule-based processing to determine how to act in the event of an unusual situation on the network.
15. A, B. Network sniffers and NIDSs are used to monitor network traffic. Network sniffers are manually oriented, whereas an NIDS can be automated.
16. C. A host-based IDS (HIDS) is installed on each host that needs IDS capabilities.
17. C. Dynamically changing the system's configuration to protect the network or a system is an active response.

18. A. By comparing attack signatures and audit trails, a misuse-detection IDS determines whether an attack is occurring.

19. D. The analyzer function uses data sources from sensors to analyze and determine whether an attack is under way.

20. A. A honeypot is a system that is intended to be sacrificed in the name of knowledge. Honeypot systems allow investigators to evaluate and analyze the attack strategies used. Law enforcement agencies use honeypots to gather evidence for prosecution.

Chapter 5: Access Control and Identity Management

Access Control and Identity Management

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **1.2 Apply and implement secure network administration principles.**
  - Firewall rules
  - VLAN management
  - Secure router configuration
  - Access control lists
  - Implicit deny
- ✓ **1.3 Distinguish and differentiate network design elements and compounds.**
  - NAC
- ✓ **3.2 Analyze and differentiate among types of attacks.**
  - Transitive access
  - Client-side attacks
- ✓ **5.1 Explain the function and purpose of authentication services.**
  - RADIUS
  - TACACS
  - TACACS+
  - Kerberos
  - LDAP
  - XTACACS

✓ **5.2 Explain the fundamental concepts and best practices related to authentication, authorization, and access control.**

- Identification vs. authentication
- Authentication (single factor) and authorization
- Multifactor authentication
- Tokens
- Common access card
- Personal identification verification card
- Smart card
- Single sign on
- ACLs
- Access control
- Mandatory access control
- Discretionary access control
- Role/rule-based access control
- Implicit deny
- Trusted OS

While the previous chapters focused more on theoretical concepts than purchasable components, they created the foundation on which the topics in this chapter will build. In this chapter, the discussion moves more into the implementation of security features as opposed to focusing only on what potential problems exist. Bear in mind that even though a variety of products exist to satisfy every need of the market, none are as successful as they should be without education and training. One of your top priorities should always be to make certain your users understand every aspect of the security policies.

This chapter starts by looking at the basics of access control and then looks at remote access and authentication services. It concludes by examining access control implementation and best practices.

Access Control Basics

Quite simply, access control means allowing the correct users in (those who are authorized) and keeping the others out (those who are not authorized). You can employ a great many tools and technologies to make this happen—all of which are discussed in this chapter—but the fundamental principle remains the same: Let the right ones in.

In the following sections, we will look at the difference between identification and authentication, authentication and authorization, multifactor authentication, and operational security. We will also look at tokens and problems to watch for as well as issues to consider.

Identification vs. Authentication

Critical to correctly answering questions asked on the Security+ exam about access control is understanding the difference between identification and authentication. Identification requires a human to intercede and verify that someone is who they say they are. The human, often in the form of a guard or receptionist, can look at the credentials the user provides (think driver's license, employee ID card, etc.) and validate that they belong with the person possessing them.

Authentication is not as fail proof as identification because it removes the human element from the verification process and merely corroborates that the user has entered the correct values, such as the password provided going with the username entered. With authentication, the user may not be who they are supposed to be, but they have indeed given the correct combination of values (such as username and password, tokens, or biometrics) and thus they are authenticated.

For the exam, remember that authentication means someone has accurate information, while identification means the accurate information is proven to be in possession of the correct individual.

Authentication systems or methods are based on one or more of these three factors:

- Something you know, such as a password or PIN
- Something you have, such as a smart card, token, or an identification device
- Something physically unique to you, such as your fingerprints or retinal pattern

Systems authenticate each other using similar methods. Frequently, systems pass private information between each other to establish identity. Once authentication has occurred, the two systems can communicate in the manner specified in the design.

Several common methods are used for authentication, and they fall within the categories of either single factor or multifactor. Each offers something to security and should be considered when you're evaluating authentication schemes or methods.

Authentication (Single Factor) and Authorization

The most basic form of authentication is known as *single factor authentication (SFA)* because only one set of values is checked. SFA is most often implemented as the traditional username/password combination. A *username* and *password* are unique identifiers for a logon process. Here's a synopsis for how it works: When users sit down in front of a computer system, the first thing a security system requires is that they establish who they are. Identification is typically confirmed through a logon process. Most operating systems use a user ID and password to accomplish this. These values can be sent across the connection as plain text or can be encrypted.

The logon process identifies to the operating system, and possibly the network, that you are who you say you are. Figure 5.1 illustrates this logon and password process. Notice that the operating system compares this information to the stored information from the security processor and either accepts or denies the logon attempt. The operating system might establish privileges or permissions based on stored data about that particular ID.

Whenever two or more parties authenticate each other, this is known as *mutual authentication*. A client may authenticate to a server and a server authenticate to a client when there is a need to establish a secure session between the two and employ encryption. Mutual authentication ensures that the client is not unwittingly connecting and giving its credentials to a rogue server, which can then turn around and steal the data from the real server.

Commonly, mutual authentication will be implemented when the data to be sent during the session is of a critical nature, such as financial or medical records.

Multifactor Authentication

When two or more access methods are included as part of the authentication process, you're implementing a *multifactor* system. A system that uses smart cards and passwords

is referred to as a *two-factor authentication* system. Two-factor authentication is shown in Figure 5.2. This example requires both a smart card and a logon password process.

FIGURE 5.1 A logon process occurring on a workstation

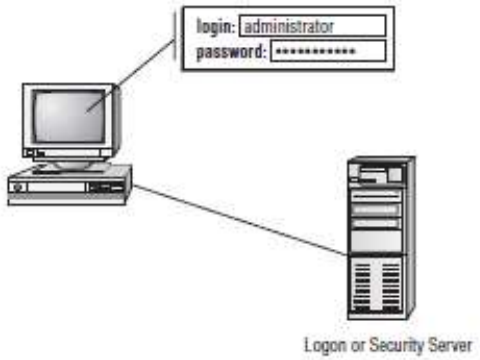
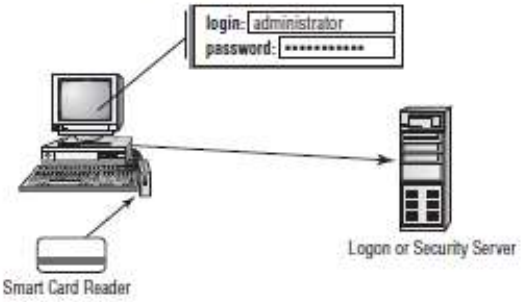


FIGURE 5.2 Two-factor authentication



Both factors must be valid:
•User ID and Password
•Smart Card

A multifactor system can consist of a two-factor system, three-factor system, and so on. As long as more than one factor is involved in the authentication process, it is considered a multifactor system.

For obvious reasons, the two or more factors employed should not be from the same category. While you do increase difficulty in gaining system accessing by requiring the user to

enter two sets of username/password combinations, it is much preferred to pair a single username/password combination with a biometric identifier or other check.

Operational Security

Operational security focuses on how an organization achieves its goals. It is also part of a security triad that includes physical and management security.

As such, operational security issues include *network access control (NAC)*, authentication, and security topologies after the network installation is complete. Issues include the daily operations of the network, connections to other networks, backup plans, and recovery plans. In short, operational security encompasses everything that isn't related to design or physical security in your network. Instead of focusing on the physical components where the data is stored, such as the server, the focus is now on the topology and connections.

Some vendors use the acronym NAC to signify network *admission* control rather than the more commonly accepted network *access* control. Regardless of which word appears in the middle of the acronym, the concept is the same.

The issues you address in an operational capacity can seem overwhelming at first. Many of the areas you'll focus on are vulnerabilities in the systems you use or weak or inadequate security policies. For example, if you implement a comprehensive password expiration policy, you can require users to change their passwords every 30 or 60 days. If the system doesn't require password rotation, though (it allows the same passwords to be reused), you have a vulnerability that you may not be able to eliminate. A user can go through the motions of changing their password only to reenter the same value and keep it in use.

From an operational perspective, this type of system has weak password-changing capabilities. There is nothing you can do, short of installing a higher-security logon process or replacing the operating system. Either solution may not be feasible given the costs, conversion times, and possible unwillingness of an organization—or its partners—to make this switch.

Such dependence on a weak system usually stems from the fact that most companies use software that was developed by third parties in order to save costs or meet compatibility requirements. These packages may require the use of a specific operating system. If that operating system has significant security problems or vulnerabilities, your duties will be mammoth because you'll still be responsible for providing security in that environment. Your secure corporate network, for example, should never be connected to the Internet, where it can become subject to a seemingly endless number of potential vulnerabilities. You must install hardware and software solutions to improve security, and you must convince management that these measures are worth the cost to implement.

Tokens

Security tokens are similar to certificates. They contain the rights and access privileges of the token bearer as part of the token. Think of a token as a small piece of data that holds a sliver of information about the user. The term *claimant* is used for a subscriber to a credential service provider.

Many operating systems generate a token that is applied to every action taken on the computer system. If your token doesn't grant you access to certain information, then either that information won't be displayed or your access will be denied. The authentication system creates a token every time a user connects or a session begins. At the completion of a session, the token is destroyed. Figure 5.3 shows the security token process.

FIGURE 5.3 Security token authentication

Potential Authentication and Access Problems

There are two problem areas you should know for the Security+ exam because they apply to authentication/access issues: transitive access and client-side attacks. Both of these are addressed in the sections that follow.

Transitive Access

The word *transitive* means involving transition, and it is necessary to understand this process in order to follow how transitive access problems occur. With *transitive access*, one party (A) trusts another party (B). If the second party (B) trusts another party (C), then a relationship can exist where the third party (C) is trusted by the first party (A).

In early operating systems, this process was often exploited. In current operating systems, such as Windows Server 2008, the problems with transitive access were solved by creating transitive trusts, which are a type of relationship that can exist between domains (the opposite is *nontransitive*). When the trust relationship is transitive, the relationship between party (A) and party (B) flows through as described earlier (i.e., A now trusts C). In all versions of Active Directory, the default is that all domains in a forest trust each other with two-way transitive trust relationships.

While this process makes administration much easier when you add a new child domain (no administrative intervention is required to establish the trusts), it leaves open

the possibility of a hacker acquiring more trust than they should by virtue of joining the domain. In Exercise 5.1, we'll explore how to validate the trust relationship in Windows Server 2008—a step toward addressing this problem.

EXERCISE 5.1

Validate a Trust Relationship

As an administrator, you should know what trust relationships exist between domains. To validate a trust relationship in Windows Server 2008, follow these steps:

1. Open Active Directory Domains and Trusts.
2. Right-click your domain name and choose Properties from the menu.
3. Click the Trusts tab and select the name of the domain, or forest, that you want to validate.
4. Click Properties. The Properties dialog box for that trust appears.
5. Approximately two-thirds of the way down the dialog box, the Transitivity Of Trust item appears. Click Validate.
6. A confirmation message appears. Click OK.
7. Exit Active Directory Domains and Trusts.

Client-Side Attacks

A *client-side attack* is an attack that targets vulnerabilities in client applications that interact with a malicious server. A user accesses the trusted site—whether web, FTP, or almost anything else—and unwittingly downloads the rogue code (thinking they are downloading music, videos, etc.). The rogue code allows the miscreant to then install or execute programs on the affected machine remotely. What is relevant to the discussion on access is that the newly installed programs run with the privilege level of the individual who accessed the server.

If that user had elevated privileges—a junior administrator, for example—then the malware runs at that level. In most cases, the programs running try to reach beyond the workstation they are initially installed on and find their way to the server(s). Often data accessed along the way is pushed out across the Internet, using HTTPS to encrypt it and make it less likely to be detected. HTTPS and Secure HTTP are discussed in Chapter 8.

Authentication Issues to Consider

You can set up many different parameters and standards to force the people in your organization to conform. In establishing these parameters, it's important that you consider the capabilities of the people who will be working with these policies. If you're working in an environment where people aren't computer savvy, you may spend a lot of time helping them

remember and recover passwords. Each organization has its own quirks, and many have had to reevaluate their security guidelines only after they've already invested great time and expense to implement high-security systems to accommodate them. Remember that it is always better to educate users—raise their awareness—than to lower security.

Setting authentication security, especially for supporting users, can become a high-maintenance activity for network administrators. On one hand, you want people to be able to authenticate themselves easily; on the other hand, you want to establish security that protects your company's resources. Here are some tips to making this process easier:

- Be wary of popular names or current trends that make certain passwords predictable. For example, every January, Super Bowl teams become likely passwords, as do variations on players' names and numbers. This can create a security problem for computer centers.
- Use *identity proofing* whenever an issue arises between identification and authentication. The identification process starts when a user ID or logon name is typed into a sign-on screen. Authentication is accomplished by challenging the claim about who is accessing the resource.
- Incorporate a second value—such as mother's maiden name—to prove a user's identity. This is helpful when identification proofing is invoked when a person claims they are the user but cannot be authenticated—such as when they lose their password.

Real World Scenario

Multifactor Authentication and Security

The CEO of your company is becoming increasingly concerned about computer security and the laxness of users. She reports that users are regularly leaving the office at the end of the day without signing out of their accounts. The company is attempting to win a contract that involves working with the government and that will require additional security measures. What would you suggest?

First and foremost, you should recommend that the company implement a multifactor authentication system. This system could consist of a smart card and a logon/password process. Most smart card readers can be configured to require that the card remain inserted in the reader while the user is logged on. If the smart card is removed, say at the end of the day, the workstation will automatically log the user out. By requiring a logon/password process, you can still provide security if the smart card is stolen. This solution provides reasonable security, and it doesn't significantly increase security costs.

Other suggestions are to consider additional access controls, such as perimeter alarms and physical access control to sensitive areas. The government would probably require these anyway, although these measures won't force users to log out when they leave their workstations.

An inherent problem with many identity proofing implementations is that they ask questions that someone other than the user could easily guess or learn the value of (what color are your eyes?). To increase the difficulty of someone fraudulent proofing, you should use only questions that are more difficult to guess or implement biometrics such as voice identification. Under no circumstance should the person proofing be allowed access immediately—instead, their access information should be sent to their email account of record.

Understanding Remote Access Connectivity

One of the primary purposes for having a network is the ability to connect systems. As networks have grown, many technologies have come on the scene to make this process easier and more secure. A key area of concern relates to the connection of systems and other networks that aren't part of your network. The following sections discuss the more common protocols used to facilitate connectivity among remote systems.

Ancient History: the Serial Line Internet Protocol

Serial Line Internet Protocol (SLIP) is an older protocol that was used in early remote access environments and serves as the starting point for most remote discussions. SLIP was originally designed to connect Unix systems in a dial-up environment and supported only serial communications.

A very simple protocol, SLIP could only be used to pass TCP/IP traffic and wasn't secure or efficient. While some systems today still support SLIP, it is strictly there for legacy systems and should be avoided whenever possible.

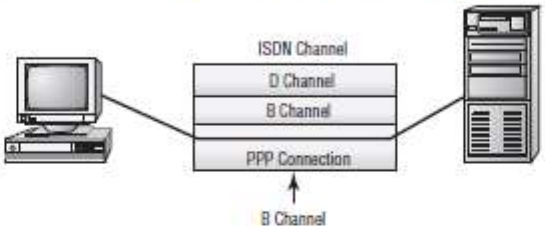
Any authentication done for a remote user is known as *remote authentication*. This authentication is commonly done using TACACS or RADIUS.

Using the Point-to-Point Protocol

Introduced in 1994, the *Point-to-Point Protocol (PPP)* offers support for multiple protocols, including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP doesn't provide data security, but it does provide authentication using the *Challenge Handshake Authentication Protocol (CHAP)*.

Figure 5.4 shows a PPP connection over an ISDN line. In the case of ISDN, PPP would normally use one 64Kbps B channel for transmission. PPP allows many channels in a network connection (such as ISDN) to be connected or bonded together to form a single virtual connection.

FIGURE 5.4 PPP using a single B channel on an ISDN connection



PPP works by encapsulating the network traffic in a protocol called the *Network Control Protocol (NCP)*. Authentication is handled by the *Link Control Protocol (LCP)*. A PPP connection allows remote users to log on to the network and have access as though they were local users on the network. PPP doesn't provide for any encryption services for the channel.

As you might have guessed, the unsecure nature of PPP makes it largely unsuitable for WAN connections. To counter this issue, other protocols have been created that take advantage of PPP's flexibility and build on it. You should make sure all your PPP connections use secure channels, dedicated connections, or high-speed connections.

Remote users who connect directly to a system don't necessarily need to have encryption capabilities enabled. If the connection is direct, the likelihood that anyone would be able to tap an existing phone line is relatively small. However, you should make sure that connections through a network use an encryption-oriented tunneling system.

Working with Tunneling Protocols

Tunneling protocols add a capability to the network: the ability to create tunnels between networks that can be more secure, support additional protocols, and provide virtual paths between systems. The best way to think of tunneling is to imagine sensitive data being encapsulated in other packets that are sent across the public network. Once they're received at the other end, the sensitive data is stripped from the other packets and recompiled into its original form.

The most common protocols used for tunneling are as follows:

Point-to-Point Tunneling Protocol *Point-to-Point Tunneling Protocol (PPTP)* supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. After the negotiation is performed,

the channel is encrypted. This is one of the major weaknesses of PPTP. A *packet-capture device*, such as a sniffer, that captures the negotiation process can potentially use that information to determine the connection type and information about how the tunnel works. Microsoft developed PPTP and supports it on most of the company's products. PPTP uses port 1723 and TCP for connections.

Layer 2 Forwarding *Layer 2 Forwarding (L2F)* was created by Cisco as a method of creating tunnels primarily for dial-up connections. It's similar in capability to PPP and shouldn't be used over WANs. L2F provides authentication, but it doesn't provide encryption. L2F uses port 1701 and TCP for connections.

Layer 2 Tunneling Protocol Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: *Layer 2 Tunneling Protocol (L2TP)*. L2TP is a hybrid of PPTP and L2F. It's primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP, so it can be used as a bridge across many types of systems. The major problem with L2TP is that it doesn't provide data security: The information isn't encrypted. Security can be provided by protocols such as IPSec. L2TP uses port 1701 and UDP for connections.

Secure Shell *Secure Shell (SSH)* is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent programs for such Unix standards as Telnet, FTP, and many other communications-oriented applications. SSH is now available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext-oriented programs in the Unix environment. SSH uses port 22 and TCP for connections.

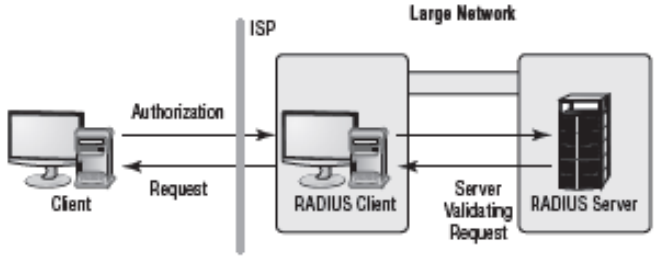
Internet Protocol Security *Internet Protocol Security (IPSec)* isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with remote connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security. IPSec can work in either Tunneling mode or Transport mode. In Tunneling mode, the data or payload and message headers are encrypted. Transport mode encrypts only the payload. IPSec is an add-on to IPv4 and built into IPv6.

Working with RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a mechanism that allows authentication of remote and other network connections. Once intended for use on dial-up connections, it has moved far beyond that and has many modern features. The RADIUS protocol is an IETF standard, and it has been implemented by most of the major operating system manufacturers. A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.

Figure 5.5 shows an example of a RADIUS server communicating with an ISP to allow access to a remote user. Notice that the remote server is functioning as a client to the RADIUS server. This allows centralized administration of access rights.

FIGURE 5.5 The RADIUS client manages the local connection and authenticates against a central server.



You should use RADIUS when you want to improve network security by implementing a single service to authenticate users who connect remotely to the network. Doing so gives you a single source for the authentication to take place. Additionally, you can implement auditing and accounting on the RADIUS server.

The major difficulty with a single-server RADIUS environment is that the entire network may refuse connections if the server malfunctions. Many RADIUS systems allow multiple servers to be used to increase reliability. All of these servers are critical components of the infrastructure, and they must be protected from attack.

TACACS/TACACS+/XTACACS

Terminal Access Controller Access-Control System (TACACS) is a client-server-oriented environment, and it operates in a manner similar to how RADIUS operates. Extended TACACS (XTACACS) replaced the original and combined authentication and authorization with logging to enable auditing.

The most current method or level of TACACS is TACACS+, and this replaces the previous two incarnations. TACACS+ allows credentials to be accepted from multiple methods, including Kerberos. The TACACS client/server process occurs in the same manner as the RADIUS process illustrated in Figure 5.5.

Cisco has widely implemented TACACS+ for connections. TACACS+ is expected to become widely accepted as an alternative to RADIUS.

Remember, RADIUS and TACACS can be used to authenticate connections.

VLAN Management

A *virtual local area network (VLAN)* allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access. You can also set up VLANs to control the

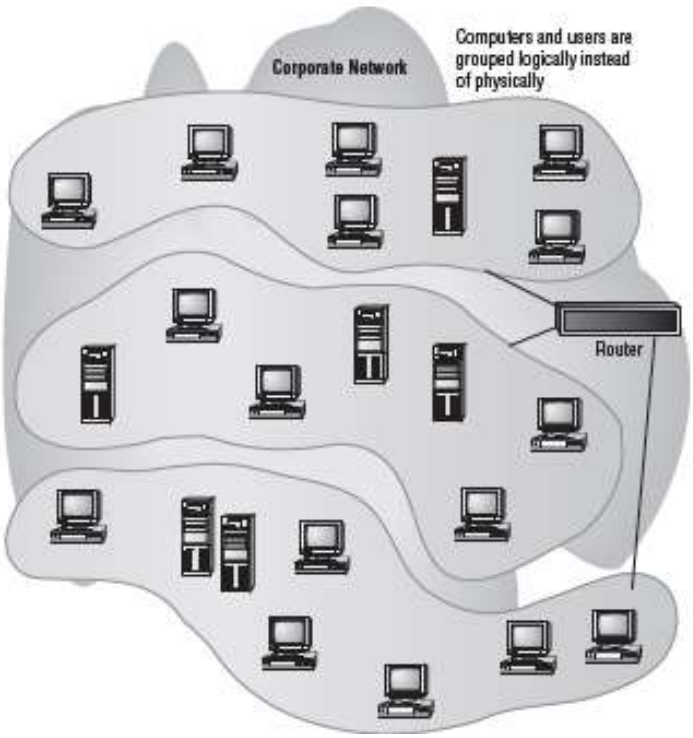
paths that data takes to get from one point to another. A VLAN is a good way to contain network traffic to a certain area in a network.

Think of a VLAN as a network of hosts that act as if they're connected by a physical wire even though there is no such wire between them.

On a LAN, hosts can communicate with each other through broadcasts, and no forwarding devices, such as routers, are needed. As the LAN grows, so too does the number of broadcasts. Shrinking the size of the LAN by segmenting it into smaller groups (VLANs) reduces the size of the broadcast domains. The advantages of doing this include reducing the scope of the broadcasts, improving performance and manageability, and decreasing dependence on the physical topology. From the standpoint of this exam, however, the key benefit is that VLANs can increase security by allowing users with similar data sensitivity levels to be segmented together.

Figure 5.6 illustrates the creation of three VLANs in a single network.

FIGURE 5.6 A typical segmented VLAN



Understanding Authentication Services

Authentication services are the implementation of the technology in question. For this part of exam study, the focus is on LDAP and Kerberos, though many other possibilities exist, such as Internet Authentication Service (IAS) and Central Authentication Service (CAS), which are outside the scope of this exam. Single sign-on initiatives round out the discussion in this section.

LDAP

Lightweight Directory Access Protocol (LDAP) is a standardized directory access protocol that allows queries to be made of directories (specifically, pared-down X.500-based directories). If a directory service supports LDAP, you can query that directory with an LDAP client, but it's LDAP that is growing in popularity and is being used extensively in online white and yellow pages.

LDAP is the main access protocol used by Active Directory (discussed next). It operates, by default, at port 389. The LDAP syntax uses commas between names.

Kerberos

Kerberos is an authentication protocol named after the mythical three-headed dog that stood at the gates of Hades. Originally designed by MIT, Kerberos is very popular as an authentication method. It allows for a single sign-on to a distributed network.

Kerberos authentication uses a *key distribution center (KDC)* to orchestrate the process. The KDC authenticates the *principal* (which can be a user, a program, or a system) and provides it with a ticket. After this ticket is issued, it can be used to authenticate against other principals. This occurs automatically when a request or service is performed by another principal.

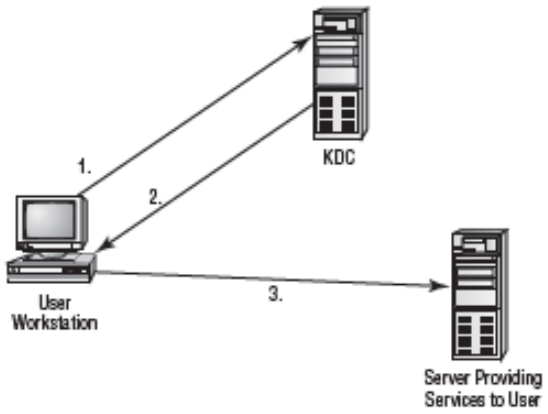
Kerberos is quickly becoming a common standard in network environments. Its only significant weakness is that the KDC can be a single point of failure. If the KDC goes down, the authentication process will stop. Figure 5.7 illustrates the Kerberos authentication process and the ticket being presented to systems that are authorized by the KDC.

The implementation of Kerberos is discussed in Chapter 9.

Single Sign-On Initiatives

One of the big problems that larger systems must deal with is the need for users to access multiple systems or applications. This may require a user to remember multiple accounts and passwords. The purpose of a *single sign-on (SSO)* is to give users access to all the applications and systems they need when they log on. This is becoming a reality in many environments, including Kerberos, Microsoft Active Directory, Novell eDirectory, and some certificate model implementations.

FIGURE 5.7 Kerberos authentication process



1. User requests access to service running on a different server.
2. KDC authenticates user and sends a ticket to be used between the user and the service on the server.
3. User's workstation sends a ticket to the service.

Single sign-on is both a blessing and a curse. It's a blessing in that once the user is authenticated, they can access all the resources on the network and browse multiple directories. It's a curse in that it removes the doors that otherwise exist between the user and various resources.

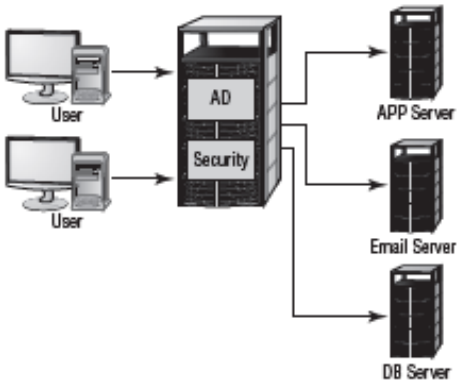
In the case of Kerberos, a single token allows any "Kerberized" applications to accept a user as valid. The important thing to remember in this process is that each application that wants to use SSO must be able to accept and process the token presented by Kerberos.

Active Directory (AD) works off a slightly different method. A server that runs AD retains information about all access rights for all users and groups in the network. When a user logs on to the system, AD issues the user a globally unique identifier (GUID). Applications that support AD can use this GUID to provide access control.

Figure 5.8 illustrates this process in more detail. In this instance, the database application, email client, and printers all authenticate with the same logon. Like Kerberos, this process requires all the applications that want to take advantage of AD to accept AD controls and directives.

In this way, the user doesn't have to have separate sign-on, email, and application passwords. Using AD simplifies the sign-on process for users and lowers the support requirements for administrators. Access can be established through groups, and it can be enforced through group memberships.

FIGURE 5.8 AD validating a user



On a decentralized network, SSO passwords are stored on each server and can represent a security risk. It's important to enforce password changes and make certain passwords are updated throughout the organization on a frequent basis.

While single sign-on is not the opposite of multifactor authentication, it is often mistakenly thought of that way. One-, two-, and three-factor authentication merely refers to the number of items a user must supply to authenticate. Authentication can be based on something they have (a smart card), something they know (a password), something unique (biometric), and so forth. After factor authentication is done, then single sign-on can still apply throughout the user's session.

Understanding Access Control

The three primary methods of access control are as follows:

Mandatory Access Control (MAC) All access is predefined.

Discretionary Access Control (DAC) Incorporates some flexibility.

Role-Based Access Control (RBAC) Allows the user's role to dictate access capabilities.

A fourth method, Rule-Based Access Control (which also uses the RBAC acronym) is gaining in popularity. Each of these methods has advantages and disadvantages to the organization from a security perspective.

The method you choose will be greatly affected by your organization's beliefs about how information needs to be shared. In a high-security environment, the tendency would be to implement either a MAC or RBAC method. In a traditional business environment or school, the tendency would be to implement a DAC method. You should do some consulting within the organization to understand how a particular department and how the entire organization want to implement access control models. Doing so will allow you to gather input from all concerned parties regarding how access guidelines should be established and how security should be implemented.

In the following sections, we'll look at each of these methods from a business perspective.

Mandatory Access Control

Mandatory Access Control (MAC) is clearly an inflexible method for how information access is allowed. In a MAC environment, all access capabilities are predefined. Users can't share information unless their rights to share it were established by administrators; administrators must make any changes that need to be made. This process enforces a rigid model of security.

For a MAC model to work effectively, administrators and network designers must think relationships through carefully. The advantage of this model is that security access is well established and defined, making security breaches easier to investigate and correct. A well-designed MAC model can make the job of information control easier and can essentially lock down a network. The major disadvantages of this model are the lack of flexibility and the fact that its needs change over time. The inability of administrative staff to address these changes can sometimes make the model hard to keep up.

This model is used in environments where confidentiality is a driving force. It often employs government and military classifications (labels) such as Top Secret and others discussed in Chapter 6.

Discretionary Access Control

In a Discretionary Access Control (DAC) model, network users have some flexibility regarding how information is accessed. This model allows users to dynamically share information with other users. The method allows a more flexible environment, but it increases the risk of unauthorized disclosure of information. Administrators have a more difficult time ensuring that information access is controlled and that only appropriate access is given out.

A classic example of DAC is the permission structure that exists for "other" with files in the Unix/Linux environment. All permissions in this operating system fall within three groups of users: owner, group, and other. The permissions associated with the owner and the group the owner belongs to are based on their roles, but all of those who are not the owner, or a member of the owner's group, fall within the category of other.

The permissions for this group are set separate from the other two and with very few special exceptions are a combination of read, write, and execute. Within this environment, I can create a database and give myself (owner) permission to read and write, give other admins (group) only read permission, and not give any permission to those not in admin (other).

I could just as easily create a script file that cleans up log files and frees space on a workstation. I would give myself (owner) all rights, give other admins (group) the ability to read and execute, and give basic users (other) the right only to execute.

Role-Based Access Control

Role-Based Access Control (RBAC) models approach the problem of access control based on established roles in an organization. RBAC models implement access by job function or by responsibility. Each employee has one or more roles that allow access to specific information. If a person moves from one role to another, the access for the previous role will no longer be available. RBAC models provide more flexibility than the MAC model and less flexibility than the DAC model. They do, however, have the advantage of being strictly based on job function as opposed to individual needs.

Instead of thinking "Denise needs to be able to edit files," RBAC uses the logic "Editors need to be able to edit files" and "Denise is a member of the Editors group." This model is always good for use in an environment in which there is high employee turnover.

Rule-Based Access Control

Rule-Based Access Control (RBAC) uses the settings in preconfigured security policies to make all decisions. These rules can be to deny all but those who specifically appear in a list (an allow list) or deny only those who specifically appear in the list (a true deny list). Entries in the list may be actual usernames, IP addresses, hostnames, or even domains. Rule-Based models are often being used in conjunction with Role-Based to add greater flexibility.

The easiest way to implement RBAC is with access control lists (ACLs), discussed later in this chapter. The ACLs create the rules by which the access control model functions.

Implementing Access Control Best Practices

How you implement access control makes all the difference in how secure your systems are. In this section, we will look at smart cards, access control lists, trusted operating systems, and secure router configuration.

Smart Cards

Smart cards are generally used for access control and security purposes. The card itself usually contains a small amount of memory that can be used to store permissions and access information.

Smart cards are difficult to counterfeit, but they're easy to steal. Once a thief has a smart card, they have all the access the card allows. To prevent this, many organizations don't put

any identifying marks on their smart cards, making it harder for someone to utilize them. A password or PIN is required to activate many modern smart cards, and encryption is employed to protect the contents. With many smart cards, if you enter the wrong pin number multiple times (usually three), the card will shut down to further enhance security.

Many European countries are beginning to use smart cards instead of magnetic-strip credit cards because they offer additional security and can contain more information.

When you think of a smart card, always remember that this tool can be used for authentication as well as storage. Not only can the card identify you, but it can hold relevant information as well. As an analogy, think of a smart card as a debit card that has an updated total of your bank account balance on it as opposed to a credit card that has only your account number.

Real World Scenario

Working with Smart Cards

You've been asked to help troubleshoot a problem that is occurring in your school's computer lab. Students are complaining about viruses that are infecting the flash drives they bring to school. How can you help remedy this situation?

You should ensure that all the systems in your school lab computers are running antivirus software and that this software is kept up-to-date. Doing so will prevent known viruses from entering the school's system and being transferred to student files. You may also want to evaluate whether the school computers should have removable media installed on their systems. Several manufacturers now sell systems called *thin clients* that don't provide any disk storage or removable media on their workstations. Thin clients use dedicated servers to download applications, data, and any other information they need to have in order to run. This eliminates the danger of viruses being introduced from student disks.

There are two main types of smart cards, which we'll discuss in the following sections.

Common Access Card

One type of smart card is the *Common Access Card (CAC)*. These cards are issued by the Department of Defense as a general identification/authentication card for military personnel, contractors, and non-DoD employees. A picture appears on the front of the card with an integrated chip beneath and a barcode. On the back of the card, there is a magnetic strip and another barcode.

The CAC is used for access to DoD computers, signing email, and implementing PKI. In 2008, the most recent year for which numbers were available, it was stated that over 17 million cards had been issued. Current information on the CAC can be found at `http://www.cac.mil`.

Personal Identification Verification Card

What the CAC is for military employees, the *Personal Identity Verification (PIV)* (referenced by CompTIA as Personal Identification Verification Card) is to federal employees and contractors. Per Homeland Security Presidential Directive number 12 (HSPD-12), the PIV will eventually be required of all U.S. Government employees and contractors. It will be required to gain access (physical and logical) to government resources.

Access Control Lists

Access control lists (ACLs) enable devices in your network to ignore requests from specified users or systems or to grant them certain network capabilities. You may find that a certain IP address is constantly scanning your network, and you can block this IP address. If you block it at the router, the IP address will automatically be rejected any time it attempts to utilize your network.

ACLs allow a stronger set of access controls to be established in your network. The basic process of ACL control allows the administrator to design and adapt the network to deal with specific security threats.

The following sections look at approaches to ACLs, including implicit deny and firewall rules.

Implicit Deny

Within ACLs, there exists a condition known as *implicit deny*. An implicit deny clause is implied at the end of each ACL and it means that if the proviso in question has not been explicitly granted, then it is denied. The best way to think of this is to use an analogy: Suppose you're hosting a party at your home and have created a guest list and given it to a bouncer at the door. When each guest arrives, the bouncer looks sequentially down the list for their name; if the name is not found on the list, then they are denied entry. You don't have to tell the bouncer to not let in Evan or Kristin or Spencer—since their names do not appear on the list, they are implicitly denied access.

The same principle holds true in the ACL. The entity being denied because it does not appear on the list can be a source address, a destination address, a packet type, or almost anything else you want to deny access.

Firewall Rules

Firewall rules act like ACLs and are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

- Block the connection.
- Allow the connection.
- Allow the connection only if it is secured.

The rules can be applied to inbound traffic or outbound traffic and any type of network (LAN, wireless, BPN, remote access). On a regular basis, you should audit the firewall rules and verify that you are obtaining the results you wish and make any modifications needed.

Trusted OS

A *trusted operating system (TOS)* is any operating system that meets the government's requirements for security. The most common set of standards for security is *Common Criteria (CC)*. This document is a joint effort among Canada, France, Germany, the Netherlands, the United Kingdom, and the United States. The standard outlines a comprehensive set of evaluation criteria, broken down into seven *Evaluation Assurance Levels (EALs)*. EAL 1 to EAL 7 are discussed here:

As of this writing, the latest version of the standard is 3.1 Release 3, and it's available for viewing at `http://www.commoncriteriaportal.org`. The website also maintains a registry of products certified by CC.

EAL 1 EAL 1 is primarily used when the user wants assurance that the system will operate correctly, but threats to security aren't viewed as serious.

EAL 2 EAL 2 requires product developers to use good design practices. Security isn't considered a high priority in EAL 2 certification.

EAL 3 EAL 3 requires conscientious development efforts to provide moderate levels of security.

EAL 4 EAL 4 requires positive security engineering based on good commercial development practices. It is anticipated that EAL 4 will be the common benchmark for commercial systems.

EAL 5 EAL 5 is intended to ensure that security engineering has been implemented in a product from the early design phases. It's intended for high levels of security assurance. The EAL documentation indicates that special design considerations will most likely be required to achieve this level of certification.

EAL 6 EAL 6 provides high levels of assurance of specialized security engineering. This certification indicates high levels of protection against significant risks. Systems with EAL 6 certification will be highly secure from penetration attackers.

EAL 7 EAL 7 is intended for extremely high levels of security. The certification requires extensive testing, measurement, and complete independent testing of every component.

EAL certification has replaced the Trusted Computer Systems Evaluation Criteria (TCSEC) system for certification, which was popular in the United States. It has also replaced the Information Technology Security Evaluation Criteria (ITSEC), which was popular in Europe. The recommended level of certification for commercial systems is EAL 4.

Currently, only a few operating systems have been approved at the EAL 4 level, and even though an operating system straight out of the box may be, that doesn't mean your own individual implementation of it is functioning at that level. If your implementation doesn't use the available security measures, then you're operating below that level.

Real World Scenario

Implementing a Secure Server Environment

You've been appointed to the panel that will make decisions regarding the purchase of a new server for your organization. The new server needs to be relatively secure and suitable for storing sensitive information. It will also be part of an e-commerce environment. How can you assist the panel?

You can be of real value to the panel by determining the operating systems that have been certified for the common criteria. You can visit the website `http://www.commoncriteriaportal.org/products/?expand #0S` to identify which operating systems and products have been EAL 4 certified. Encourage your IT staff members to make their decision based on the data available about security as opposed to vendor claims. Most vendors claim to have a secure environment when in fact they don't. The CC certification proves that an impartial third party did an evaluation.

As an administrator, you should know and thoroughly understand that just because the operating system you have is capable of being certified at a high level of security doesn't mean that your implementation is at that level.

Secure Router Configuration

One of the most important things you can do to secure your network is make sure you secure the router. As much common sense as it makes, it is too often overlooked in the hurry to get the router configuration finished and move on to the next job. To securely configure the router, you must do the following:

Change the Default Password. The password for the administrator is set before the router leaves the factory. You have to assume that every miscreant wanting unauthorized access to your network knows the default passwords set by the factory. Employ good password principles (alphanumeric, more than 8 characters, etc.) and change it to a value that only those who must know do.

Walk through the Advanced Settings. These settings will differ based on the router manufacturer and type but often include settings to block ping requests, perform MAC filtering, and so on. All of these issues are discussed elsewhere in this book and need to be applied to the router configuration the same as they would be applied elsewhere.

Keep the Firmware Upgraded. Router manufacturers often issue patches when problems are discovered. Those patches need to be applied to the router to remove any security exploits that may exist.

Always remember to back up your router configuration before making any significant changes—in particular a firmware upgrade—to provide a fallback in case something goes awry.

Cisco routers often utilize one of two different types of passwords for their accounts: Type 7 and MD5. Type 7 passwords use weak encryption and are considered only slightly above Type 0, which is cleartext. As such, Type 7 passwords are easily decrypted with readily available shareware/freeware and should be avoided. MD5 password encryption utilizes a one-way hash, and this is configured in IOS using the command **enable secret**.

Summary

The focus of this chapter was on access control and identity management. The key difference between authentication and identification is that authentication means someone has accurate information, while identification means the accurate information is proven to be in possession of the correct individual.

The most basic form of authentication is known as single factor authentication (SFA) because only one set of values is checked. To increase security, it is necessary to move to multifactor authentication, which involves two or more values that are checked.

This chapter examined the various types of authentication services in use, including RADIUS and different variations of TACACS. It also looked at tunneling protocols, smart cards, and other means of access control.

Security baselines provide a standardized method for evaluating the security capabilities of particular products. Never consider an operating system or application to be secured unless it has been certified using the EAL standard, which provides seven levels of certification. EAL 4 is the level recommended to provide reasonable security for commercial operating systems.

ACLs are being implemented in network devices and systems to enable the control of access to systems and users; ACLs allow individual systems, users, or IP addresses to be ignored.

Exam Essentials

Be able to describe the roles of access control. The three primary roles are MAC, DAC, and RBAC. Mandatory Access Control (MAC) establishes rigid access control methods in the organization. Discretionary Access Control (DAC) allows for flexibility in access control. Role-Based Access Control (RBAC) is based on the role the individual or department has in the organization. In a fourth type, Rule-Based Access Control (RBAC), settings in preconfigured security policies are used to make all decisions.

Know the characteristics of the connectivity technologies available to you and the security capabilities associated with each. Remote access, PPP, tunneling protocols, and VPNs are your primary tools. PPTP and L2TP are two of the most common protocols used for tunneling. IPSec, although not a tunneling protocol, provides encryption to tunneling protocols; it's often used to enhance tunnel security.

Know how ACLs work. Access control lists (ACLs) are used to identify systems and specify which users, protocols, or services are allowed. ACL-based systems can be used to prevent unauthorized users from accessing vulnerable services.

Explain the relative advantages of the technologies available to you for authentication. You have many tools available to establish authentication processes. Some of these tools start with a password and user ID. Others involve physical devices or the physical characteristics of the person who is requesting authentication.

Be able to identify the differences and characteristics of the technologies available to you. A network can be segmented, and VLANs can be created to improve security. NAT presents only one Internet address to the world, hiding the other elements of the network. Tunneling allows you to make relatively secure connections to other networks using the Internet.

Review Questions

1. Most of your client's sales force have been told that they should no longer report to the office on a daily basis. From now on, they're to spend the majority of their time on the road calling on customers. Each member of the sales force has been issued a laptop computer and told to connect to the network nightly through a remote connection. Which of the following protocols is widely used today as a transport protocol for remote Internet connections?
   A. SMTP
   B. PPP
   C. PPTP
   D. L2TP
2. Which protocol is unsuitable for WAN VPN connections?
   A. PPP
   B. PPTP
   C. L2TP
   D. IPSec
3. You've been given notice that you'll soon be transferred to another site. Before you leave, you're to audit the network and document everything in use and the reason why it's in use. The next administrator will use this documentation to keep the network running. Which of the following protocols isn't a tunneling protocol but is probably used at your site by tunneling protocols for network security?
   A. IPSec
   B. PPTP
   C. L2TP
   D. L2F
4. The present method of requiring access to be strictly defined on every object is proving too cumbersome for your environment. The edict has come down from upper management that access requirements should be reduced slightly. Which access model allows users some flexibility for information-sharing purposes?
   A. DAC
   B. MAC
   C. RBAC
   D. MLAC

5. A newly hired junior administrator will assume your position temporarily while you attend a conference. You're trying to explain the basics of security to her in as short a period of time as possible. Which of the following best describes an ACL?
   A. ACLs provide individual access control to resources.
   B. ACLs aren't used in modern systems.
   C. The ACL process is dynamic in nature.
   D. ACLs are used to authenticate users.

6. LDAP is an example of which of the following?
   A. Directory access protocol
   B. IDS
   C. Tiered model application development environment
   D. File server

7. Upper management has suddenly become concerned about security. As the senior network administrator, you are asked to suggest changes that should be implemented. Which of the following access methods should you recommend if the method is to be one that is primarily based on preestablished access and can't be changed by users?
   A. MAC
   B. DAC
   C. RBAC
   D. Kerberos

8. Your office administrator is being trained to perform server backups. Which authentication method would be ideal for this situation?
   A. MAC
   B. DAC
   C. RBAC
   D. Security tokens

9. You've been assigned to mentor a junior administrator and bring him up to speed quickly. The topic you're currently explaining is authentication. Which method uses a KDC to accomplish authentication for users, programs, or systems?
   A. CHAP
   B. Kerberos
   C. Biometrics
   D. Smart cards

10. After a careful risk analysis, the value of your company's data has been increased. Accordingly, you're expected to implement authentication solutions that reflect the increased value of the data. Which of the following authentication methods uses more than one authentication process for a logon?
    A. Multifactor
    B. Biometrics
    C. Smart card
    D. Kerberos

11. You're the administrator for Mercury Technical. Due to several expansions, the network has grown exponentially in size within the past two years. Which of the following is a popular method for breaking a network into smaller private networks that can coexist on the same wiring and yet be unaware of each other?
    A. VLAN
    B. NAT
    C. MAC
    D. Security zone

12. Which technology allows a connection to be made between two networks using a secure protocol?
    A. Tunneling
    B. VLAN
    C. Internet
    D. Extranet

13. Your company provides medical data to doctors from a worldwide database. Because of the sensitive nature of the data you work with, it's imperative that authentication be established on each session and be valid only for that session. Which of the following authentication methods provides credentials that are valid only during a single session?
    A. Tokens
    B. Certificate
    C. Smart card
    D. Kerberos

13. Which of the following is the term used whenever two or more parties authenticate each other?
    A. SSO
    B. Multifactor authentication
    C. Mutual authentication
    D. Tunneling

15. Which of the following security areas encompasses network access control (NAC)?
    A. Physical security
    B. Operational security
    C. Management security
    D. Triad security

16. You have added a new child domain to your network. As a result of this, the child has adopted all the trust relationships with other domains in the forest that existed for its parent domain. What is responsible for this?
    A. LDAP access
    B. XML access
    C. Fuzzing access
    D. Transitive access

17. What is invoked when a person claims they are the user but cannot be authenticated—such as when they lose their password?
    A. Identity proofing
    B. Social engineering
    C. Directory traversal
    D. Cross-site requesting

18. Which of the following is a client-server-oriented environment that operates in a manner similar to RADIUS?
    A. HSM
    B. TACACS
    C. TPM
    D. ACK

19. What is implied at the end of each access control list?
    A. Least privilege
    B. Separation of duties
    C. Implicit deny
    D. Explicit allow

20. Which of the following is a type of smart card issued by the Department of Defense as a general identification/authentication card for military personnel, contractors, and non-DoD employees?
    A. PIV
    B. POV
    C. DLP
    D. CAC

Answers to Review Questions

1. B. PPP can pass multiple protocols and is widely used today as a transport protocol for remote connections.
2. A. PPP provides no security, and all activities are unsecure. PPP is primarily intended for remote connections and should never be used for VPN connections.
3. A. IPSec provides network security for tunneling protocols. IPSec can be used with many different protocols besides TCP/IP, and it has two modes of security.
4. A. DAC allows some flexibility in information-sharing capabilities within the network.
5. A. Access control lists allow individual and highly controllable access to resources in a network. An ACL can also be used to exclude a particular system, IP address, or user.
6. A. Lightweight Directory Access Protocol (LDAP) is a directory access protocol used to publish information about users. This is the computer equivalent of a phone book.
7. A. Mandatory Access Control (MAC) is oriented toward preestablished access. This access is typically established by network administrators and can't be changed by users.
8. C. Role-Based Access Control (RBAC) allows specific people to be assigned to specific roles with specific privileges. A backup operator would need administrative privileges to back up a server. This privilege would be limited to the role and wouldn't be present during the employee's normal job functions.
9. B. Kerberos uses a key distribution center (KDC) to authenticate a principal. The KDC provides a credential that can be used by all Kerberos-enabled servers and applications.
10. A. A multifactor authentication method uses two or more processes for logon. A two-factor method might use smart cards and biometrics for logon.
11. A. Virtual local area networks (VLANs) break a large network into smaller networks. These networks can coexist on the same wiring and be unaware of each other. A router or other routing-type device would be needed to connect these VLANs.
12. A. Tunneling allows a network to make a secure connection to another network through the Internet or other network. Tunnels are usually secure and present themselves as extensions of both networks.
13. A. Tokens are created when a user or system successfully authenticates. The token is destroyed when the session is over.
14. C. Whenever two or more parties authenticate each other, this is known as mutual authentication.
15. B. Operational security issues include network access control (NAC), authentication, and security topologies after the network installation is complete.

16. D. Transitive access exists between the domains and creates this relationship.

17. A. Identity proofing is invoked when a person claims they are the user but cannot be authenticated, such as when they lose their password.

18. B. Terminal Access Controller Access-Control System (TACACS) is a client-server-oriented environment, and it operates in a manner similar to how RADIUS operates.

19. C. An implicit deny clause is implied at the end of each ACL, and it means that if the proviso in question has not been explicitly granted, then it is denied.

20. D. One type of smart card is the Common Access Card (CAC). These cards are issued by the Department of Defense as a general identification/authentication card for military personnel, contractors, and non-DoD employees.

Chapter 10: Physical and Hardware-Based Security

Physical and Hardware-Based Security

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

- ✓ **2.6 Explain the impact and proper use of environmental controls.**
  - HVAC
  - Fire suppression
  - EMI shielding
  - Hot and cold aisles
  - Environmental monitoring
  - Temperature and humidity controls
  - Video monitoring
- ✓ **3.6 Analyze and differentiate among types of mitigation and deterrent techniques.**
  - Physical security: Hardware locks; Mantraps; Video surveillance; Fencing; Proximity readers; Access list
- ✓ **4.2 Carry out appropriate procedures to establish host security.**
  - Hardware security: Cable locks; Safe; Locking cabinets
- ✓ **5.2 Explain the fundamental concepts and best practices related to authentication, authorization, and access control.**
  - Biometrics

This chapter will help you understand the importance of physical security measures such as access controls, physical barriers, and biometric systems. It also covers the environment your systems need in order to be safe and operational. This chapter also discusses securing the network, and looks at security zones and partitioning.

Physical security measures prevent your systems from being accessed in unauthorized ways, primarily by preventing an unauthorized user from physically touching a system or device. Most networked systems have developed high levels of sophistication and security from outside intruders. However, these systems are generally vulnerable to internal attacks, sabotage, and misuse. If an intruder has physical access to your systems, you should never consider them to be secure.

Implementing Access Control

Access control is a critical part of physical security. Systems must operate in controlled environments in order to be secure. These environments must be, as much as possible, safe from intrusion. Computer system consoles can be a vital point of vulnerability because many administrative functions can be accomplished from the system console. These consoles, as well as the systems themselves, must be protected from physical access. Two areas that help increase access control and make a system secure are physical barriers and biometrics, both of which are discussed in the following sections.

Physical Barriers

A key aspect of access control involves *physical barriers*. The objective of a physical barrier is to prevent access to computers and network systems. The most effective physical barrier implementations require that more than one physical barrier be crossed to gain access. This type of approach is called a *multiple barrier system*.

Ideally, your systems should have a minimum of three physical barriers:

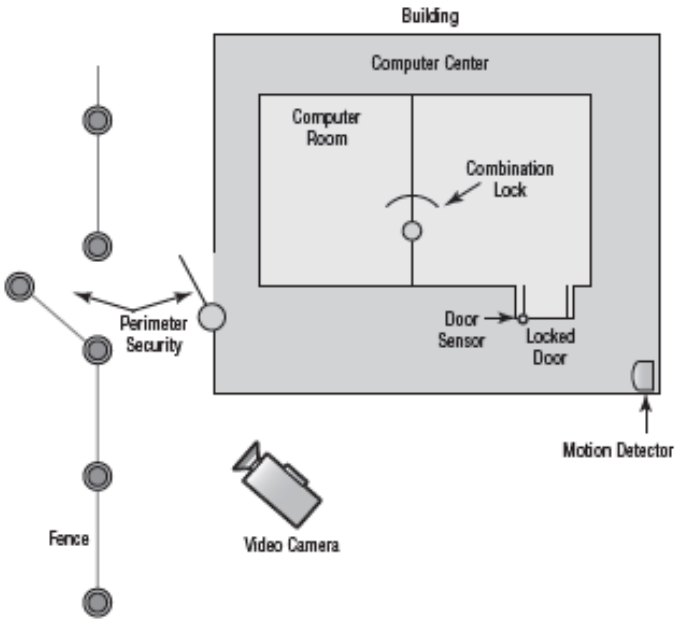
- The external entrance to the building, referred to as a *perimeter*, which is protected by burglar alarms, external walls, *fencing*, surveillance, and so on. This should be used with an *access list*, which should exist to specifically identify who can enter a facility and can be verified by a guard or someone in authority.
- A locked door protecting the computer center; you should also rely on such items as *ID badges*, fobs, or keys to gain access.

- The entrance to the computer room itself. This should be another locked door that is carefully monitored. While you try to keep as many intruders out with the other two barriers, many who enter the building could be posing as someone they are not—heating technicians, representatives of the landlord, and so on. Although these pretenses can get them past the first two barriers, they should still be stopped by the locked computer room door.

Each of these entrances can be individually secured, monitored, and protected with alarm systems. Figure 10.1 illustrates this concept.

Proximity reader is a catchall term for any ID or card reader capable of reading *proximity cards*. Proximity cards go by a number of different titles but are really just RFID (radio frequency identification) cards that can be read when close to a reader and never need to truly touch anything. The readers work with 13.56 MHz smart cards and 125 kHz proximity cards and can open turnstiles, gates, and any other physical security safeguards once the signal is read.

FIGURE 10.1 The three-layer security model



Although these three barriers won't always stop intruders, they will potentially slow them down enough that law enforcement can respond before an intrusion is fully developed. Once inside, a truly secure site should be dependent on a *physical token* or biometrics for access to the actual network resources.

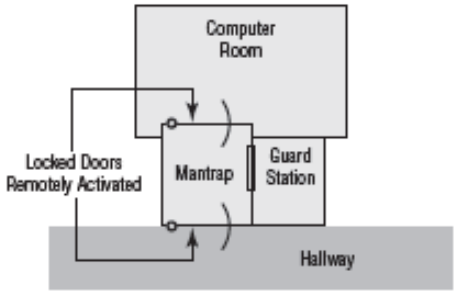
Physical tokens are anything that a user must have on them to access network resources and are often associated with devices that enable the user to generate a one-time password authenticating their identity. SecurID, from RSA, is one of the best-known examples of a physical token, and information on it can be found at `http://www.rsa.com/node.aspx?id=1156`.

No matter how secure you think your system is, you'll never be able to stop everyone. But your goal is to stop most attempts and, at the very least, slow down the most sophisticated. As an analogy, the front door of your home may contain a lock and a deadbolt. This minimal security is enough to convince most burglars to try somewhere less secure. A professional who is bent on entering your home, however, could always take a chain saw or similar tool to the door.

Mantraps

High-security installations use a type of intermediate access control mechanism called a *mantrap* (also occasionally written as *man-trap*). Mantraps require visual identification, as well as authentication, to gain access. A mantrap makes it difficult for a facility to be accessed in number because it allows only one or two people into the facility at a time. It's usually designed to physically contain an unauthorized, potentially hostile person until authorities arrive. Figure 10.2 illustrates a mantrap. Notice in this case that the visual verification is accomplished using a security guard. A properly developed mantrap includes bulletproof glass, high-strength doors, and locks. In high-security and military environments, an armed guard, as well as *video surveillance*, would be placed at the mantrap. After a person is inside the facility, additional security and authentication may be required for further entrance.

FIGURE 10.2 A mantrap in action



Some mantraps even include scales to weigh the person. While the weight can be used to help identify a person, often the scales are used to make certain no one is sneaking in. If the weight of the scale appears too high, an officer can check to make sure two people haven't crowded in and are attempting to quickly bypass security.

Perimeter Security

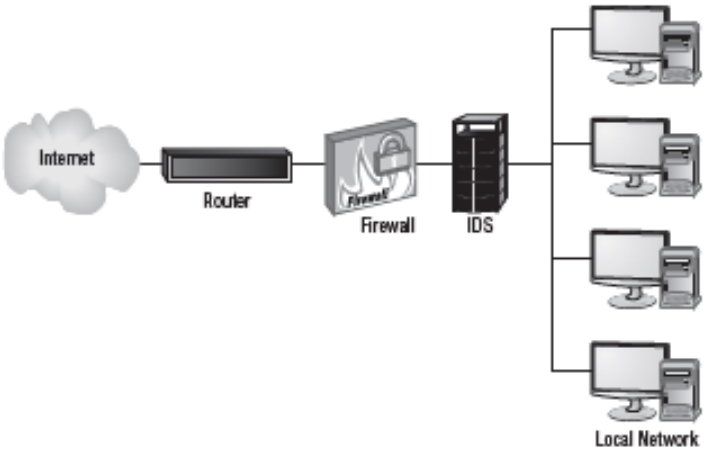
Perimeter security, whether physical or technological, is the first line of defense in your security model. In the case of a physical security issue, the intent is to prevent unauthorized access to resources inside a building or facility.

The network equivalent of physical perimeter security is intended to accomplish for a network what perimeter security does for a building. How do you keep intruders from gaining access to systems and information in the network through the network?

In the physical environment, perimeter security is accomplished using locks, doors, surveillance systems, and alarm systems. This isn't functionally any different from a network, which uses border routers, intrusion detection systems, and firewalls to prevent unauthorized access. Figure 10.3 illustrates the systems used to prevent network intrusion.

Few security systems can be implemented that don't have weaknesses or vulnerabilities. A determined intruder can, with patience, overcome most security systems. The task may not be easy, and it may require careful planning and study; however, a determined adversary can usually figure out a way. This is why deterrent factors are so important.

FIGURE 10.3 Network perimeter defense



If you want to deter intruders from breaking into your building, you can install improved door locks, coded alarm systems, and magnetic contacts on doors and windows. Remember that you can't always keep an intruder out of your building; however, you can make an intrusion riskier and more likely to be discovered if it happens.

Don't overlook the obvious. Adding a security guard to the front door will go a long way toward keeping an intruder out.

Real World Scenario

Circumventing Security

Recently, a small business noticed that the level of network traffic seemed to be very high in the late evening and early morning. The business couldn't find a network-related reason why this was happening. Upon investigation, the security consultant found that a part-time employee had established a multiuser game server in his office. The game server was set to turn on after 10:00 p.m. and turn off at 5:30 a.m. This server was hidden under a desk, and it supported around 30 local game players. The part-time employee didn't have a key to the building, so an investigation was conducted to determine how he gained access to the building after hours. The building had electronic locks on its outside entrances, and a pass card was needed to open the doors. However, the door locks were designed to automatically unlock when someone was leaving the building.

The investigation discovered that the employee and a friend had figured out a way to slide a piece of cardboard under one of the external doors, which activated the door mechanisms and unlocked the doors. The intruders took advantage of this weakness in the doors to gain access after hours without using a passcard and then used the server to play games in his office.

Hardware Security

Hardware security involves applying physical security modifications to secure the system(s) and prevent them from leaving the facility. Don't spend all your time worrying about intruders coming through the network wire and overlook the obvious need for physical security.

Adding a *cable lock* between a laptop and a desk prevents someone from picking it up and walking away with a copy of your customer database. Every laptop case I am aware of includes a built-in security slot in which a cable lock can be added to prevent it from easily being removed from the premises, like the one shown in Figure 10.4.

When it comes to desktop models, adding a lock to the back cover can prevent an intruder with physical access from grabbing the hard drive or damaging the internal components. The

lock that connects through that slot can also go to a cable that then connects to a desk or other solid fixture to keep the entire PC from being carried away. An example of this type of configuration is shown in Figure 10.5.

FIGURE 10.4 A cable in the security slot keeps the laptop from easily being removed.

FIGURE 10.5 A cable can be used to keep a desktop machine from easily being taken.

In addition to running a cable to the desk, you can also choose to run an end of it up to the monitor if theft of peripherals is a possibility. An example of this is shown in Figure 10.6.

FIGURE 10.6 If theft of equipment is a possibility, run one end of the cable from the monitor to the desktop machine through the hole in the work desk.

You should also consider using *safes* and *locking cabinets* to protect backup media, documentation, and any other physical artifacts that could do harm if they fell into the wrong hands. Server racks should lock the rack-mounted servers into the cabinets to prevent someone from simply pulling one and walking out the front door with it.

While this discussion is on physical security, don't overlook encryption as a means of increasing data security should a desktop or laptop machine be stolen. You can also consider removing the hard drives in areas that are difficult to monitor and forcing all data to be stored on the network.

Security Zones

A *security zone* is an area in a building where access is individually monitored and controlled. A large network, such as a big physical plant, can have many areas that require restricted access. In a building, floors, sections of floors, and even offices can be broken down into smaller areas. These smaller zones are referred to as security zones. In the physical environment, each floor is broken into separate zones. An alarm system that identifies a zone of intrusion can inform security personnel about an intruder's location in the building; zone notification tells security where to begin looking when they enter the premises.

The concept of security zones is as old as security itself. Most burglar alarms allow the creation of individual zones within a building or residence; these zones are then treated separately by the security staff. In a residence, it would be normal for the bedroom to be assigned a zone of its own so movement here can occur while other parts of the house may be set on a motion detector.

In Exercise 10.1, we'll walk through the evaluation of your environment.

EXERCISE 10.1

Security Zones in the Physical Environment

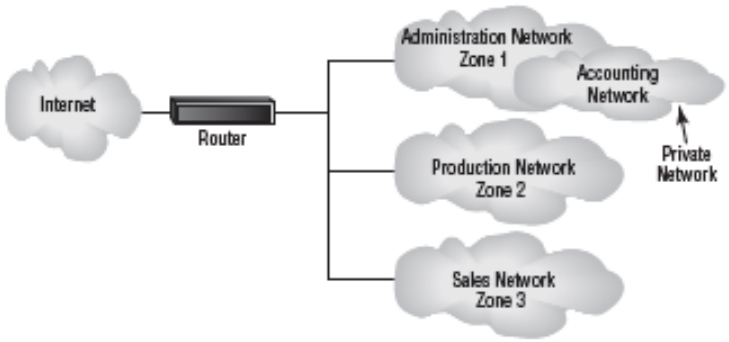
As a security administrator, you'll need to evaluate your workplace and think of physical zones that should exist in terms of different types of individuals who might be present. If your workplace is already divided into zones, forget that this has been done and start from scratch. Answer the following questions:

1. What areas represent the physical dimension of your workplace (buildings, floors, offices, and so on)?
2. Which areas are accessible by everyone from administrators to visitors? Can a visitor ever leave the reception area without an escort, and if so, to go where (restroom, break room, and so forth)?
3. In what areas are users allowed to move about freely? Are you certain that no visitors or guests could enter those areas?
4. What areas are administrators allowed to enter that users can't? Server room? Wiring closets? How do you keep users out and verify that only administrators enter?
5. Are wall jacks, network access, or Wi-Fi available in areas where visitors are located?
6. Do other areas need to be secured for entities beyond the user/administrator distinction (such as groups)?

Once you're armed with this information, you should look for ways to address the weaknesses. You should evaluate your environment routinely to make certain the zones that exist within your security plan are still relevant. Always start from scratch and pretend that no zones exist; then verify that the zones that do exist are the same as those you've created from this exercise.

The networking equivalent of a security zone is a network security zone. They perform the same function. If you divide a network into smaller sections, each zone can have its own security considerations and measures—just like a physical security zone. Figure 10.7 illustrates a larger network being broken down into three smaller zones. Notice that the first zone also contains a smaller zone where high-security information is stored. This arrangement allows layers of security to be built around sensitive information. The division of the network is accomplished by implementing virtual LANs (VLANs) and instituting demilitarized zones (DMZs).

FIGURE 10.7 Network security zones



Partitioning

Partitioning a network is functionally the same as partitioning a building. In a building, walls exist to direct pedestrian flow, provide access control, and separate functional areas. This process allows information and property to be kept under physical lock and key.

Through partitioning, you can isolate one entity from another. That entity can be physical (one room can be shut from another in a building) or logical (those who can access one set of data cannot access another). This discussion will elaborate on the possibilities partitioning provides.

Partitions can be either temporary or permanent structures.

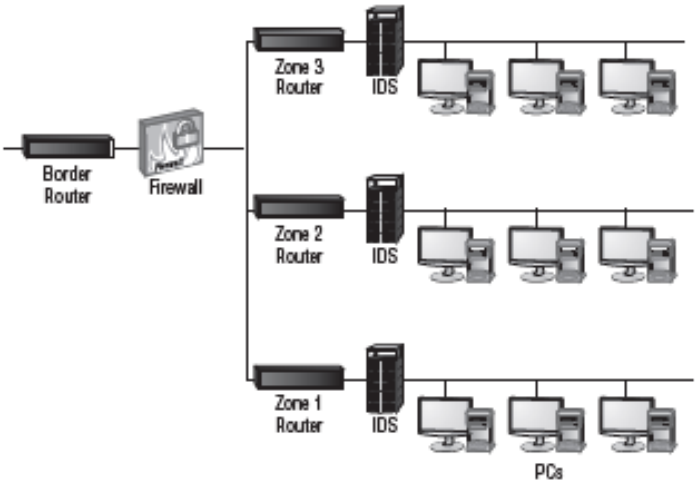
Hallways in an office building are usually built differently from internal office space. Hallways are usually more flame resistant, and they're referred to as *fire corridors*. These corridors allow people in the building to escape in the event of a fire. Fire corridor walls go from the floor to the ceiling, whereas internal walls can stop before they reach the ceiling (most office buildings have a false ceiling in them to hold lighting, wiring, and plumbing).

Network partitioning accomplishes the same function for a network as physical partitioning does for a building. Buildings have physical walls, whereas network partitioning involves the creation of private networks within larger networks. Partitions can be isolated from each other using routers and firewalls.

Therefore, while the network systems are all connected using wire, the functional view is that of many smaller networks. Figure 10.8 shows a partitioned network. It's important to realize that unless a physical device (such as a router) separates these partitioned networks, all the signals are shared across the wire. This device accomplishes the same function as a hallway or locked door—from a purely physical perspective.

Partitioning and security zones are essentially interchangeable. Typically, partitioning is more narrowly focused than zones, but this need not always be the case. In a typical installation, a zone would encompass one floor, while a partition would include one room.

FIGURE 10.8 Network partitioning separating networks from each other in a larger network



Real World Scenario

Installing Biometric Devices

You've been asked to solve the problem of people forgetting the smart cards that give them access to the computer center. Hardly a day goes by that a company employee doesn't forget to bring their card. This can cause a great deal of disruption in the workplace because someone has to constantly reissue smart cards. The company has tried everything it can think of short of firing people who forget their cards. What could you recommend to the company?

Investigate whether biometric devices (such as hand scanners) or number access locks can be used in lieu of smart cards for access. These devices will allow people who forget their smart cards to enter areas that they should be able to access.

Biometrics

Biometric systems use some kind of unique biological trait to identify a person, such as fingerprints, patterns on the retina, and handprints. Some of the devices that are used are hand scanners, retinal scanners, facial recognition applications, and keystroke recognition programs, which can be used as part of the access control mechanisms. These devices should be coupled into security-oriented computer systems that record all access attempts. They should also be under surveillance in order to prevent individuals from bypassing them.

These technologies are becoming more reliable, and they will become widely used over the next few years. Many laptops sold now have a fingerprint reader built in. The costs associated with these technologies have fallen drastically in recent years. One of the best independent sources of information on development in the field of biometrics is BiometricNews.net, where you can find links to publications and their blog.

Real World Scenario

Evaluating Your Security System

You've been asked to evaluate your building's security system. The president chose you because you understand computers, and after all, these new alarm systems are computerized.

In evaluating the environment, you notice that there is a single control panel for the whole building. A few motion detectors are located in the main hallway. Beyond that, no additional security components are installed.

This situation is fairly normal in a small building. You could recommend enhancing the system by adding motion detectors in each major hallway. You could also install *video monitoring* (also known as surveillance) cameras, such as closed-circuit television (CCTV), at all the entrances. Most security/surveillance CCTV cameras have PTZ (Pan, Tilt, and Zoom) capabilities to and can often do so based on sound or motion. You should also consider recommending they upgrade the perimeter security by adding contact sensors on all the doors and ground-floor windows.

Always evaluate the building from a multi-tiered approach. Incorporate as many different elements as you can where needed: perimeter security, security zones, and surveillance.

Maintaining Environmental and Power Controls

The location of your computer facility is critical to its security. Computer facilities must be placed in a location that is physically possible to secure. Additionally, the location must have the proper capabilities to manage temperature, humidity, and other environmental

factors necessary to the health of your computer systems. The following sections look at environmental and power systems.

Environmental Monitoring

Many computer systems require *temperature and humidity control* for reliable service. The larger servers, communications equipment, and drive arrays generate considerable amounts of heat; this is especially true of mainframe and older minicomputers. An environmental system for this type of equipment is a significant expense beyond the actual computer system costs. Fortunately, newer systems operate in a wider temperature range. Most new systems are designed to operate in an office environment.

If the computer systems you're responsible for require special environmental considerations, you'll need to establish cooling and humidity control. Ideally, systems are located in the middle of the building, and they're ducted separately from the rest of the *HVAC* (Heating, Ventilation, and Air Conditioning) system. It's a common practice for modern buildings to use a zone-based air conditioning environment, which allows the environmental plant to be turned off when the building isn't occupied. A computer room will typically require full-time environmental control.

Environmental systems should be monitored to prevent the computer center's humidity level from dropping below 50 percent. Electrostatic damage is likely to occur when humidity levels get too low.

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock. Most environmental systems also regulate humidity; however, a malfunctioning system can cause the humidity to be almost entirely extracted from a room. Make sure that environmental systems are regularly serviced.

Environmental concerns also include considerations about water and flood damage as well as fire suppression. Computer rooms should have fire and moisture detectors. Most office buildings have water pipes and other moisture-carrying systems in the ceiling. If a water pipe bursts (which is common in minor earthquakes), the computer room could become flooded. Water and electricity don't mix. Moisture monitors would automatically kill power in a computer room if moisture were detected, so the security professional should know where the water cutoffs are located.

Fire, no matter how small, can cause damage to computer systems. Apart from the high heat, which can melt or warp plastics and metals, the smoke from the fire can permeate the computers. Smoke particles are large enough to lodge under the read/write head of a hard disk, thereby causing data loss. In addition, the fire-suppression systems in most buildings consist of water under pressure, and the water damage from putting out even a small fire could wipe out an entire data center.

Fire suppression is discussed further in this chapter in the section by the same name, "Fire Suppression."

The three critical components of any fire are heat, fuel, and oxygen. If any component of this trilogy is removed, a fire isn't possible. Most fire-suppression systems work on this concept.

Power Systems

Computer systems are susceptible to power and interference problems. A computer requires a steady input of AC power to produce reliable DC voltage for its electronic systems. *Power systems* are designed to operate in a wide band of power characteristics; they help keep the electrical service constant, and they ensure smooth operations.

Real World Scenario

Simple Things Can Have Huge Consequences

Water can come from anywhere, and you need to be prepared when it does. Several years ago, a business had a state-of-the-art server room on the top floor of its building. The room was climate controlled and a true thing of beauty. Directly above the server room was the roof, and on the roof was the bank of air conditioners for the six-floor building. Over the course of one extremely hot weekend, the drain lines for the condensation from the air conditioners clogged. The lines filled with water and then burst, and the water came through the roof into the attic. Once in the attic, all the water worked its way to the lowest spot and created a hole in the ceiling—directly above the servers. Everything was fried in a short period of time.

As far-fetched as it sounds, such things happen all the time. When they do, you need to be ready with backups—backup tapes, backup servers, backup monitors, and so on.

Major fluctuations in AC power can contribute to a condition known as *chip creep*. With creep, unsoldered chips slowly work their way loose and out of a socket over time.

The following products solve most electrical line problems:

Surge Protectors *Surge protectors* protect electrical components from momentary or instantaneous increases (called *spikes*) in a power line. Most surge protectors shunt a voltage spike to ground through the use of small devices called *metal oxide varistors (MOVs)*. Large-scale surge protectors are usually found in building power supplies or at power-feed points in the building. Portable surge protectors can be purchased as part of an extension cord or power

strip but are often good for only one good hit. If subsequent surges occur, the surge protector may not prevent them from being passed through the line to the computer system. Surge protectors are passive devices, and they accomplish no purpose until a surge occurs.

Power Conditioners *Power conditioners* are active devices that effectively isolate and regulate voltage in a building. They monitor the power in the building and clean it up. Power conditioners usually include filters, surge suppressors, and temporary voltage regulation. They can also activate backup power supplies. Power conditioners can be part of the overall building power scheme; it's also common to see them dedicated strictly to computer rooms.

Backup Power *Backup power* is generally used in situations where continuous power is needed in the event of a power loss. These types of systems are usually designed for either short-term, as in the case of a battery backup system, or long-term uses, as in an *uninterruptible power supply (UPS)*. UPS systems generally use batteries to provide short-term power. Longer-term backup power comes from power generators that frequently have their own power-loss-sensing circuitry. Power generators kick in if a power loss is detected, and they provide power until disabled. The generators require a short amount of time to start providing power, and the battery backup systems provide time for the generators to come online. Most generator systems don't automatically turn off when power is restored to a building—they're turned off manually. This is necessary because it's common for several false starts to occur before power is restored from the power grid.

Most power generators are either gas or diesel operated, and they require preventive maintenance on a regular basis. These systems aren't much use if they don't start when needed or they fail because no oil is in the motor. Newer systems are becoming available that are based on fuel cell technology; they will probably be very reliable and require less maintenance.

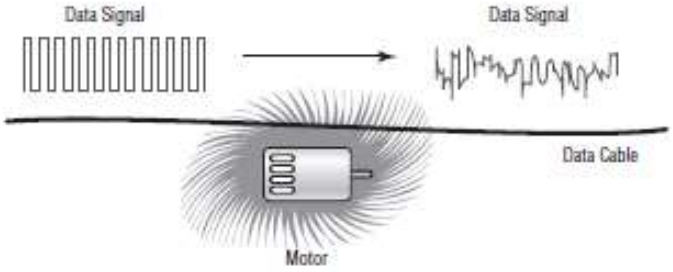
EMI Shielding

Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. In a fixed facility, such as a computer center, surrounding the computer room with a *Faraday cage* can provide electronic shielding. A Faraday cage usually consists of an electrically conductive wire mesh or other conductor woven into a "cage" that surrounds a room. The conductor is then grounded. Because of this cage, few electromagnetic signals can either enter or leave the room, thereby reducing the ability to eavesdrop on a computer conversation. In order to verify the functionality of the cage, radio frequency (RF) emissions from the room are tested with special measuring devices.

Electromagnetic interference (EMI) and *radio frequency interference (RFI)* are two additional environmental considerations. Motors, lights, and other types of electromechanical objects cause EMI, which can cause circuit overload, spikes, or electrical component failure. Making sure that all signal lines are properly shielded and grounded can minimize EMI. Devices that generate EMI should be as physically distant from cabling as is feasible because this type of energy tends to dissipate quickly with distance.

Figure 10.9 shows a motor generating EMI. In this example, the data cable next to the motor is picking up the EMI. This causes the signal to deteriorate, and it might eventually cause the line to be unusable. The gray area in the illustration is representative of the interference generated by the motor.

FIGURE 10.9 Electromagnetic interference (EMI) pickup in a data cable

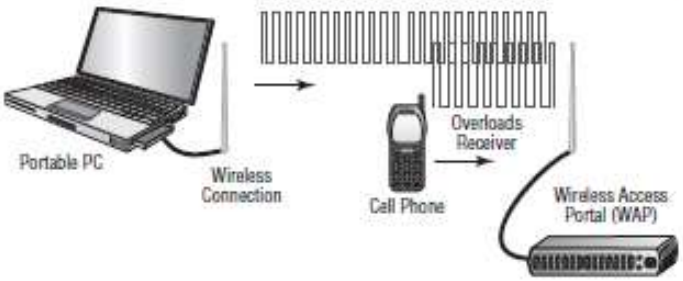


RFI is the byproduct of electrical processes, similar to EMI. The major difference is that RFI is usually projected across a radio spectrum. Motors with defective brushes can generate RFI, as can a number of other devices. If RF levels become too high, it can cause the receivers in wireless units to become deaf. This process is called *desensitizing*, and it occurs because of the volume of RF energy present. This can occur even if the signals are on different frequencies.

Figure 10.10 demonstrates the desensitizing process occurring with a wireless access portal (WAP). The only solutions in this situation would be to move the devices farther apart or to turn off the RFI generator.

In 1985, Dutch researcher Wim van Eck proposed that it is possible to eavesdrop on CRT and LCD displays by detecting their electromagnetic emissions. Known as *Van Eck phreaking*, this problem/possibility has been in the news recently because of potential problems with electronic voting machines. Commonly associated countermeasures recommended by TEMPEST include shielding.

FIGURE 10.10 RF desensitization occurring as a result of cellular phone interference



Project TEMPEST

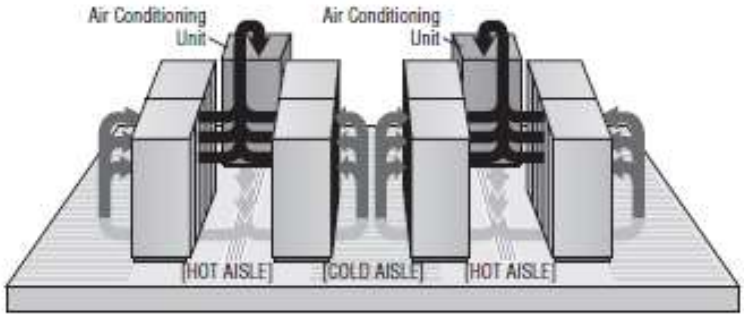
TEMPEST is the name of a project commenced by the U.S. government in the late 1960s. TEMPEST was concerned with reducing electronic noise from devices that would divulge intelligence about systems and information. This program has become a standard for computer systems certification. *TEMPEST shielding protection* means that a computer system doesn't emit any significant amounts of EMI or RFI. For a device to be approved as a TEMPEST, it must undergo extensive testing, done to exacting standards that the U.S. government dictates. Today, control zones and white noise are used to accomplish the shielding. TEMPEST-certified equipment frequently costs twice as much as non-TEMPEST equipment.

Hot and Cold Aisles

In server rooms, there are often multiple rows of servers located in racks. The rows of servers are known as aisles, and they can be cooled as *hot aisles* and *cold aisles*. With a hot aisle, hot air outlets are used to cool the equipment, while with cold aisles, cold air intake is used to cool it. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation.

It is important that the hot air exhausting from one aisle of racks not be the intake air pulled in by the next row of racks, or overheating will occur. Air handlers must move the hot air out, while cold air, usually coming from beneath a raised floor, is supplied as the intake air. Figure 10.11 shows an example of a hot and cold aisle design.

FIGURE 10.11 Example of a hot and cold aisle design



Fire Suppression

Fire suppression is a key consideration in computer-center design. Fire suppression is the act of actually extinguishing a fire versus preventing one. Two primary types of fire-suppression systems are in use: fire extinguishers and fixed systems.

Fire Extinguishers

Fire extinguishers are portable systems. The selection and use of fire extinguishers is critical. Four primary types of fire extinguishers are available, classified by the types of fires they put out: A, B, C, and D. Table 10.1 describes the four types of fires and the capabilities of various extinguishers.

TABLE 10.1 Fire Extinguisher Ratings

Type	Use	Retardant Composition
A	Wood and paper	Largely water or chemical
B	Flammable liquids	Fire-retardant chemicals
C	Electrical	Nonconductive chemicals
D	Flammable metals	Varies, type specific

A type K extinguisher that is marketed for use with cooking oil fires can also be found in stores. In actuality, this is a subset of class B extinguishers.

Several multipurpose types of extinguishers combine extinguisher capabilities in a single bottle. The more common multipurpose extinguishers are A-B, B-C, and ABC.

The recommended procedure for using a fire extinguisher is called the *PASS method*: pull, aim, squeeze, and sweep. Fire extinguishers usually operate for only a few seconds—if you use one, make sure you don't fixate on a single spot. Most fire extinguishers have a limited effective range of from three to eight feet.

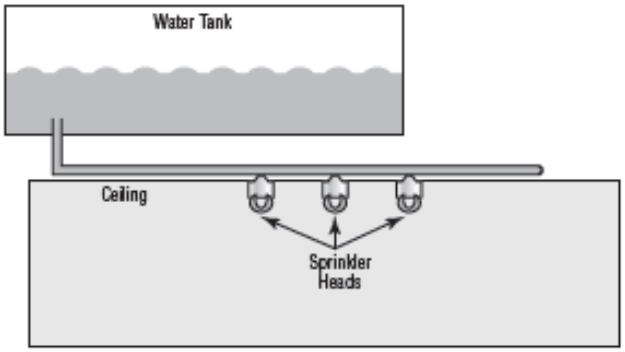
A major concern with electrical fires is that they can reoccur quickly if the voltage isn't removed. Make sure you remove voltage from systems when a fire occurs.

Most fire extinguishers require an annual inspection. This is a favorite area of citation by fire inspectors. You can contract with services to do this on a regular basis: They will inspect or replace your fire extinguishers according to a scheduled agreement.

Fixed Systems

Fixed systems are usually part of the building systems. The most common fixed systems combine fire detectors with fire-suppression systems, where the detectors usually trigger either because of a rapid temperature change or because of excessive smoke. The fire-suppression system uses either water sprinklers or fire-suppressing gas. Water systems work with overhead nozzles, as illustrated in Figure 10.12. These systems are the most common method in modern buildings. Water systems are reliable, relatively inexpensive, and require little maintenance.

FIGURE 10.12 Water-based fire-suppression system



The one drawback to water-based systems is that they cause extreme damage to energized electrical equipment such as computers. These systems can be tied into relays that terminate power to computer systems before they release water into the building.

Gas-based systems were originally designed to use carbon dioxide and later halon gas. Halon gas isn't used anymore because it damages the ozone layer; environmentally acceptable substitutes are now available, with FM 200 being one of the most common. The principle of a gas system is that it displaces the oxygen in the room, thereby removing this necessary component of a fire.

Evacuate the room immediately in the event of a fire. Gas-based systems work by removing oxygen from the fire, and this can suffocate anyone in the room as well.

The major drawback to gas-based systems is that they require sealed environments to operate. Special ventilation systems are usually installed in gas systems to limit air circulation when the gas is released. Gas systems are also expensive, and they're usually implemented only in computer rooms or other areas where water would cause damage to technology or other intellectual property.

Summary

In this chapter, I covered the key elements of physical security and the environment. Physical security measures include access controls, physical barriers, and environmental systems. Environmental considerations include electrical, fire-suppression, and interference issues.

Security models must be concerned with physical security, security zones, partitioning, and the communications infrastructure. You should take a multilayered approach when you implement a security model.

Exam Essentials

Know the various aspects of physical security. Physical security involves mechanisms to provide access control, physical barriers, and authentication systems such as biometric systems.

Be able to describe the types of access control methods used in physical security. The primary methods of access control include perimeter security, security zones, physical barriers, and identification systems. These systems, when implemented in layers, make it harder for an intruder to gain access. Physical access methods should also include intrusion detection systems such as video surveillance in order to monitor the activities when they occur. This helps security professionals manage the threat and make changes when necessary.

Be able to discuss the various aspects of environmental systems and functions. Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant.

Know the purposes of shielding in the environment. Shielding primarily prevents interference from EMI and RFI sources. Most shielding is attached to an effective ground, thereby neutralizing or reducing interference susceptibility.

Be able to describe the types of fire-suppression systems in use today. Fire-suppression systems can be either fixed or portable. Portable systems usually are fire extinguishers. Fixed systems are part of the building, and they're generally water based or gas based. Gas-based systems are usually found only in computer rooms or other locations where water-based systems would cause more damage than is warranted. Gas systems work only in environments where airflow can be limited; they remove oxygen from the fire, causing the fire to go out. Water systems usually remove heat from a fire, causing the fire to go out.

Review Questions

1. Which component of physical security addresses outer-level access control?
   - **A.** Perimeter security
   - **B.** Mantraps
   - **C.** Security zones
   - **D.** Locked doors
2. You've been drafted for the safety committee. One of your first tasks is to inventory all the fire extinguishers and make certain the correct types are in the correct locations throughout the building. Which of the following categories of fire extinguisher is intended for use on electrical fires?
   - **A.** Type A
   - **B.** Type B
   - **C.** Type C
   - **D.** Type D
3. Which of the following won't reduce EMI?
   - **A.** Physical shielding
   - **B.** Humidity control
   - **C.** Physical location
   - **D.** Overhauling worn motors
4. You're the administrator for MTS. You're creating a team that will report to you, and you're attempting to divide the responsibilities for security among individual members. Similarly, which of the following access methods breaks a large area into smaller areas that can be monitored individually?
   - **A.** Zone
   - **B.** Partition
   - **C.** Perimeter
   - **D.** Floor
5. Which of the following is equivalent to building walls in an office building from a network perspective?
   - **A.** Perimeter security
   - **B.** Partitioning
   - **C.** Security zones
   - **D.** IDS systems

6. After a number of minor incidents at your company, physical security has suddenly increased in priority. No unauthorized personnel should be allowed access to the servers or workstations. The process of preventing access to computer systems in a building is called what?
   - **A.** Perimeter security
   - **B.** Access control
   - **C.** Security zones
   - **D.** IDS systems

7. Which of the following is an example of perimeter security?
   - **A.** Chain link fence
   - **B.** Video camera
   - **C.** Elevator
   - **D.** Locked computer room

8. You're the leader of the security committee at ACME. After a move to a new facility, you're installing a new security monitoring system throughout. Which of the following best describes a motion detector mounted in the corner of a hallway?
   - **A.** Perimeter security
   - **B.** Partitioning
   - **C.** Security zone
   - **D.** IDS system

9. Which technology uses a physical characteristic to establish identity?
   - **A.** Biometrics
   - **B.** Surveillance
   - **C.** Smart card
   - **D.** CHAP authenticator

10. The process of reducing or eliminating susceptibility to outside interference is called what?
    - **A.** Shielding
    - **B.** EMI
    - **C.** TEMPEST
    - **D.** Desensitization

11. You work for an electronics company that has just created a device that emits less RF than any competitor's product. Given the enormous importance of this invention and of the marketing benefits it could offer, you want to have the product certified. Which certification is used to indicate minimal electronic emissions?
    - **A.** EMI
    - **B.** RFI
    - **C.** CC EAL 4
    - **D.** TEMPEST

12. Due to growth beyond current capacity, a new server room is being built. As a manager, you want to make certain that all the necessary safety elements exist in the room when it's finished. Which fire-suppression system works best when used in an enclosed area by displacing the air around a fire?
    A. Gas based
    B. Water based
    C. Fixed system
    D. Overhead sprinklers

13. Type K fire extinguishers are intended for use on cooking oil fires. This type is a subset of which other type of fire extinguisher?
    A. Type A
    B. Type B
    C. Type C
    D. Type D

14. Proximity readers work with which of the following? (Choose all that apply.)
    A. 15.75 fob card
    B. 14.32 surveillance card
    C. 13.56 MHZ smart card
    D. 125 kHz proximity card

15. In a hot and cold aisle system, what is the typical method of handling cold air?
    A. It is pumped in from below raised floor tiles.
    B. It is pumped in from above through the ceiling tiles.
    C. Only hot air is extracted and cold air is the natural result.
    D. Cold air exists in each aisle.

16. If RF levels become too high, it can cause the receivers in wireless units to become deaf. This process is called:
    A. Clipping
    B. Desensitizing
    C. Distorting
    D. Crackling

17. RFI is the byproduct of electrical processes, similar to EMI. The major difference is that RFI is usually projected across which of the following?
    A. Network medium
    B. Electrical wiring
    C. Radio spectrum
    D. Portable media

18. For physical security, what should you do with rack-mounted servers?
    A. Run a cable from them to a desk.
    B. Lock each of them into the cabinet.
    C. Install them in safes.
    D. Use only Type D, which incorporates its own security.
19. Which of the following is a method of cooling server racks in which hot air and cold are both handled in the server room?
    A. Hot/cold vessels
    B. Hot and cold passages
    C. Hot/cold walkways
    D. Hot and cold aisles
20. Which of the following is a high-security installation that requires visual identification, as well as authentication, to gain access?
    A. Mantrap
    B. Fencing
    C. Proximity reader
    D. Hot aisle

Answers to Review Questions

1. A. The first layer of access control is perimeter security. Perimeter security is intended to delay or deter entrance into a facility.
2. C. Type C fire extinguishers are intended for use in electrical fires.
3. B. Electrical devices, such as motors, that generate magnetic fields cause EMI. Humidity control won't address EMI.
4. A. A security zone is a smaller part of a larger area. Security zones can be monitored individually if needed. Answers B, C, and D are examples of security zones.
5. B. Partitioning is the process of breaking a network into smaller components that can each be individually protected. This is analogous to building walls in an office building.
6. B. Access control is the primary process of preventing access to physical systems.
7. A. Perimeter security involves creating a perimeter or outer boundary for a physical space. Video surveillance systems wouldn't be considered a part of perimeter security, but they can be used to enhance physical security monitoring.
8. C. A security zone is an area that is a smaller component of the entire facility. Security zones allow intrusions to be detected in specific parts of the building.
9. A. Biometrics is a technology that uses personal characteristics, such as a retinal pattern or fingerprint, to establish identity.
10. A. Shielding keeps external electronic signals from disrupting operations.
11. D. TEMPEST is the certification given to electronic devices that emit minimal RF. The TEMPEST certification is difficult to acquire, and it significantly increases the cost of systems.
12. A. Gas-based systems work by displacing the air around a fire. This eliminates one of the three necessary components of a fire: oxygen.
13. B. Type K fire extinguishers are a subset of Type B fire extinguishers.
14. C, D. Proximity readers work with 13.56 MHz smart card and 125 kHz proximity cards.
15. A. With hot and cold aisles, cold air is pumped in from below raised floor tiles.
16. B. If RF levels become too high, it can cause the receivers in wireless units to become deaf and is known as desensitizing. This occurs because of the volume of RF energy present.
17. C. RFI is the byproduct of electrical processes, similar to EMI. The major difference is that RFI is usually projected across a radio spectrum. Motors with defective brushes can generate RFI, as can a number of other devices.

18. B. Server racks should lock the rack-mounted servers into the cabinets to prevent someone from simply pulling one and walking out the front door with it.

19. D. Hot and cold aisles is a method of cooling server racks in which hot air and cold are both handled in the server room.

20. A. High-security installations use a type of intermediate access control mechanism called a mantrap. Mantraps require visual identification, as well as authentication, to gain access. A mantrap makes it difficult for a facility to be accessed in number because it allows only one or two people into the facility at a time.

Chapter 12: Wireless Networking Security

Wireless Networking Security

THE FOLLOWING COMPTIA SECURITY+ EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **1.6 Implement wireless network in a secure manner.**

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC filter
- SSID broadcast
- TKIP
- CCMP
- Antenna Placement
- Power level controls

✓ **3.4 Analyze and differentiate among types of wireless attacks.**

- Rogue access points
- Interference
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking

Wireless systems, plainly put, are systems that don't use wires to send information but rather transmit data through the air. The growth of wireless systems creates several opportunities for attackers. These systems are relatively new, they use well-established communications mechanisms, and they're easily intercepted.

This chapter discusses the various types of wireless systems that you'll encounter and mentions some of the security issues associated with this technology. Specifically, the systems deal with Wireless Transport Layer Security (WTLS), the IEEE 802 wireless standards, WPA2, WEP/WAP applications, and the vulnerabilities that each presents.

Working with Wireless Systems

The days of coax running through the room are past. More and more, we are moving to an environment where wireless is *the* networking topology of choice. To make that environment successful, and to pass the CompTIA exam, you need to understand the 802.11 standards that are applicable, as well as the technologies—the implementations of those standards—in use today.

This section looks at the protocols you need to know, as well as the transport layer implementation.

IEEE 802.11*x* Wireless Protocols

The *IEEE 802.11x* family of protocols provides for wireless communications using radio frequency transmissions. The frequencies in use for 802.11 standards are the 2.4GHz and the 5GHz frequency spectrum. Several standards and bandwidths have been defined for use in wireless environments, and—with the exception of 802.11a—tend to be compatible with each other:

802.11 The *802.11* standard defines wireless LANs transmitting at 1Mbps or 2Mbps bandwidths using the 2.4GHz frequency spectrum and using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) for data encoding.

802.11a The *802.11a* standard provides wireless LAN bandwidth of up to 54 Mbps in the 5GHz frequency spectrum. The 802.11a standard also uses orthogonal frequency division multiplexing (OFDM) for encoding rather than FHSS or DSSS.

802.11b The *802.11b* standard provides for bandwidths of up to 11 Mbps (with fallback rates of 5.5, 2, and 1 Mbps) in the 2.4GHz frequency spectrum. This standard

is also called *Wi-Fi* or *802.11 high rate*. The 802.11b standard uses only DSSS for data encoding.

802.11g The *802.11g* standard provides for bandwidths of up to 54 Mbps in the 2.4GHz frequency spectrum. While able to obtain faster speeds, it also suffers from the same interference problems inherent with 802.11b—having to share the spectrum with other devices using that frequency.

802.11i The *802.11i* standard provides for security enhancements to the wireless standard with particular focus on authentication. The standard is often referenced as WPA2, the name given it by the Wi-Fi Alliance.

802.11n The *802.11n* standard provides for bandwidths of up to 300 Mbps in the 5GHz frequency spectrum (it can also communicate at 2.4GHz for compatibility). The advantage of this standard is that it offers higher speed and a frequency that does not have as much interference.

Most of the time, a wireless access point will work with more than one 802.11 standard. In Figure 12.1, for example, the Dell Wireless WLAN Card Utility shows that most of the networks this client is able to pick up a signal from are using 802.11b, 802.11g, and 802.11n.

FIGURE 12.1 A number of wireless networks are found, and most are using more than one 802.11 standard

Three technologies are used to communicate in the 802.11 standard and provide backward compatibility with 802.11b:

Direct-Sequence Spread Spectrum *Direct-sequence spread spectrum (DSSS)* accomplishes communication by adding the data that is to be transmitted to a higher-speed transmission. The higher-speed transmission contains redundant information to ensure data accuracy. Each packet can then be reconstructed in the event of a disruption.

Frequency-Hopping Spread Spectrum *Frequency-hopping spread spectrum (FHSS)* accomplishes communication by hopping the transmission over a range of predefined frequencies. The changing or hopping is synchronized between both ends and appears to be a single transmission channel to both ends.

Orthogonal Frequency Division Multiplexing *Orthogonal frequency division multiplexing (OFDM)* accomplishes communication by breaking the data into sub-signals and transmitting them simultaneously. These transmissions occur on different frequencies or sub-bands.

The mathematics and theories of these transmission technologies are beyond the scope of this book.

WEP/WAP/WPA/WPA2

Wired Equivalent Privacy (WEP) was intended to provide basic security for wireless networks, while wireless systems frequently use the Wireless Application Protocol (WAP) for network communications. Over time, WEP has been replaced in most implementations by WPA and WPA2. The following sections briefly discuss these terms and provide you with an understanding of their relative capabilities.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a wireless protocol designed to provide privacy equivalent to that of a wired network. WEP is implemented in a number of wireless devices, including PDAs and cell phones. WEP is vulnerable because of weaknesses in the way the encryption algorithms (RC4) are employed. These weaknesses allow the algorithm to potentially be cracked in as few as five minutes using available PC software. This makes WEP one of the more vulnerable protocols available for security.

As an example, the initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it is easy for miscreants to crack the WEP secret key; this is known as an *IV attack*. To put it in perspective, the attack happens because the algorithm used is RC4, the IV is too small, the IV is static, and the IV is part of the RC4 encryption key.

Figure 12.2 shows the configuration settings on a very simple wireless router and sums up the situation best: The only time to use WEP is when you must have compatibility with older devices that do not support new encryption.

To make the encryption stronger, *Temporal Key Integrity Protocol (TKIP)* was employed. This places a 128-bit wrapper around the WEP encryption with a key that is based on such things as the MAC address of your machine and the serial number of the packet. TKIP was

designed as a backward-compatible replacement to WEP and could use all existing hardware. Without the use of TKIP, WEP—as mentioned earlier in this chapter—is considered weak. It is worth noting, however, that even TKIP has been broken.

FIGURE 12.2 Wireless security settings for a simple router

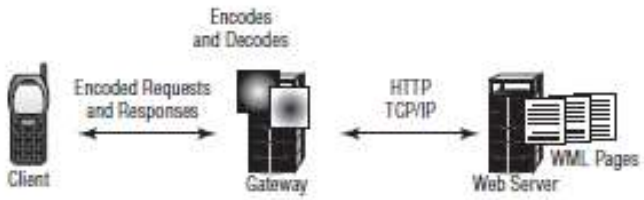
Wireless Application Protocol

The Wireless Application Protocol (WAP) is the technology designed for use with wireless devices. WAP has become a standard adopted by many manufacturers, including Motorola and Nokia. WAP functions are equivalent to TCP/IP functions in that they're trying to serve the same purpose for wireless devices. WAP uses a smaller version of HTML called *Wireless Markup Language (WML)*, which is used for Internet displays. WAP-enabled devices can also respond to scripts using an environment called *WMLScript*. This scripting language is similar to Java, which is a programming language.

The ability to accept web pages and scripts produces the opportunity for malicious code and viruses to be transported to WAP-enabled devices. No doubt this will create a new set of problems, and antivirus software will be needed to deal with them.

WAP systems communicate using a WAP gateway system, as depicted in Figure 12.3. The gateway converts information back and forth between HTTP and WAP as well as encodes and decodes between the protocols.

FIGURE 12.3 A WAP gateway enabling a connection to WAP devices by the Internet



This structure provides a reasonable assurance that WAP-enabled devices can be secured. If the interconnection between the WAP server and the Internet isn't encrypted, packets between the devices may be intercepted (which is referred to as *packet sniffing*), creating a potential vulnerability. This vulnerability is called a *gap in the WAP* (the security concern that exists when converting between WAP and SSL/TLS) and was prevalent in versions of WAP prior to 2.0.

Wi-Fi Protected Access and WPA2

The *Wi-Fi Protected Access (WPA)* and Wi-Fi Protected Access 2 (WPA2) technologies were designed to address the core problems with WEP. These technologies were created to implement the 802.11i standard. The difference between WPA and WPA2 is that the former implements most—but not all—of 802.11i in order to be able to communicate with older wireless cards (which might still need an update through their firmware in order to be compliant) and it used the RC4 encryption algorithm with TKIP, while WPA2 implements the full standard and is not compatible with older cards.

WPA also mandates the use of TKIP, while WPA2 favors *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*. CCMP uses 128-bit AES encryption with a 48-bit initialization vector. With the larger initialization vector, it increases the difficulty in cracking and minimizes the risk of replay.

As a simplified timeline useful for exam study, think of WEP as coming first. It was fraught with errors and WPA (with TKIP) was used as an intermediate solution, implementing a portion of the 802.11i standard. The final solution—a full implementation of the 802.11i standard—is WPA2 (with CCMP).

Wireless Transport Layer Security

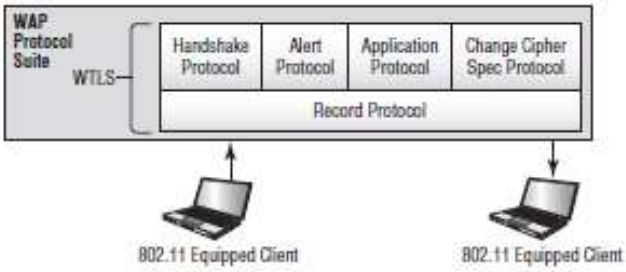
Wireless Transport Layer Security (WTLS) is the security layer of the Wireless Application Protocol, discussed in the section "WEP/WAP/WPA/WPA2." WTLS provides authentication, encryption, and data integrity for wireless devices. It's designed to utilize the relatively narrow bandwidth of these types of devices and is moderately secure. WTLS provides reasonable security for mobile devices, and it's being widely implemented in wireless devices.

Wireless Transport Layer Security provides an encrypted and authenticated connection between a wireless client and a server. WTLS is similar in function to TLS, but it uses a lower bandwidth and less processing power. It's used to support wireless devices, which don't yet have extremely powerful processors.

Figure 12.4 illustrates WTLS as part of the WAP environment. WAP provides the functional equivalent of TCP/IP for wireless devices. Many devices, including newer cell phones and PDAs, include support for WTLS as part of their networking protocol capabilities.

Communication between a WAP handset and WAP server is protected by WTLS. Once on the Internet, a connection is typically protected by the Secure Socket Layer (SSL), an Internet standard for encrypting data between points on the network.

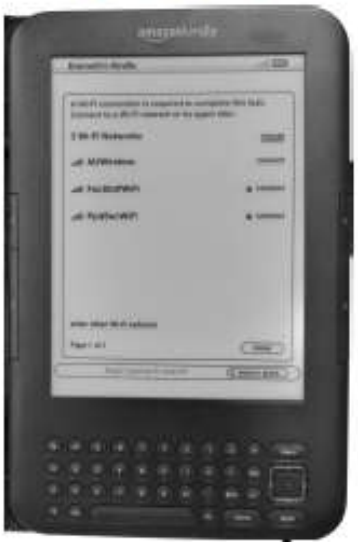
FIGURE 12.4 WTLS used between two WAP devices



Understanding Mobile Devices

Mobile devices, including smartphones, e-readers, tablet computers, and personal digital assistants (PDAs), are popular. Many of these devices use either RF signaling or cellular technologies for communication. Figure 12.5, for example, shows an Amazon Kindle looking for wireless networks.

FIGURE 12.5 Wireless scanning is done by a wide variety of devices such as the Kindle.



If the device uses the Wireless Application Protocol (WAP), the device in all likelihood doesn't have security enabled. Several levels of security exist in WAP:

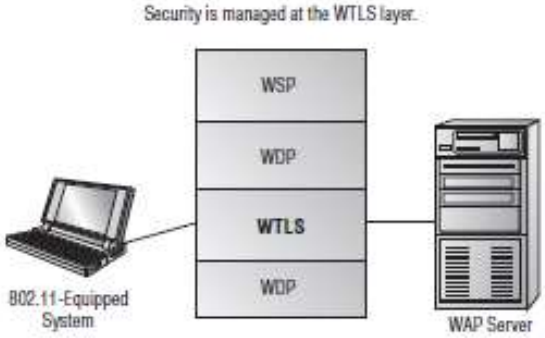
Anonymous Authentication This allows virtually anyone to connect to the wireless portal.

Server Authentication This requires the workstation to authenticate against the server.

Two-Way (Client and Server) Authentication This requires both ends of the connection (client and server) to authenticate to confirm validity.

Many new wireless devices are also capable of using certificates to verify authentication. Figure 12.6 shows a mobile systems network; this network uses both encryption and authentication to increase security.

FIGURE 12.6 A mobile environment using WAP security



The following are the technologies used to provide services between the devices:

Wireless Session Protocol (WSP) This manages the session information and connection between the devices.

Wireless Transaction Protocol (WTP) This provides services similar to TCP and UDP for WAP.

Wireless Datagram Protocol (WDP) This provides the common interface between devices.

Wireless Transport Layer Security (WTLS) This is the security layer of the Wireless Application Protocol.

Wireless Access Points

It does not take much to build a wireless network. On the client side, you need a wireless network interface card (NIC) in place of the standard wired NIC. On the network side, you need something to communicate with the clients.

The primary method of connecting a wireless device to a network is via a wireless portal. A *wireless access point* (commonly just called an access point or AP) is a low-power transmitter/receiver, also known as a *transceiver*, which is strategically placed for access. The portable device and the access point communicate using one of several communications protocols, including *IEEE 802.11* (also known as Wi-Fi).

Wireless communications, as the name implies, don't use wires as the basis for communication. Most frequently, they use a portion of the *radio frequency (RF)* spectrum called *microwave*. Wireless communication methods are becoming more prevalent in computing because the cost of the transmitting and receiving equipment has fallen drastically over the last few years. Wireless also offers mobile connectivity within a campus, a building, or even a city. Most wireless frequencies are shared frequencies in that more than one person may be using the same frequency for communication.

Figure 12.7 illustrates a wireless portal being used to connect a computer to a company network. Notice that the portal connects to the network and is treated like any other connection used in the network.

Wireless communications, although convenient, can also be less than secure. While many APs now ship with encryption turned on, you will still want to verify that this is the case with your network. In Figure 12.1, it is possible to see that bsu and bsuguest are not utilizing security. Figure 12.8 shows a received packet from an unsecure network, while Figure 12.9 shows the information received from a network that has security enabled. Notice the list of protocols in the lower half of Figure 12.9.

FIGURE 12.7 Wireless access portal and workstation

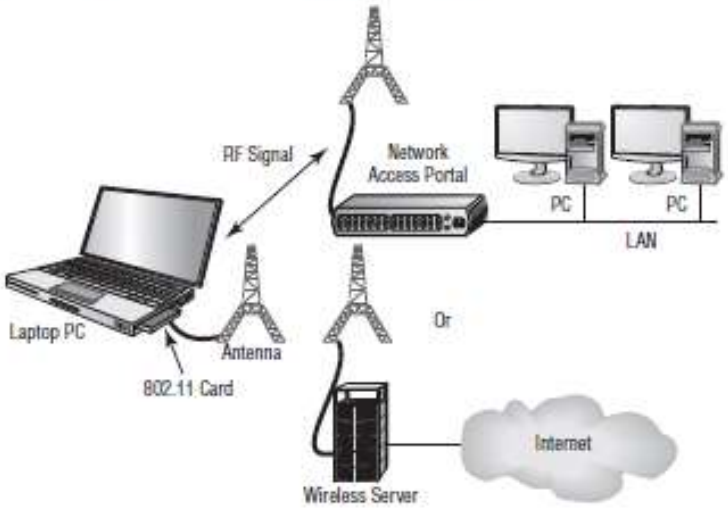


FIGURE 12.8 Data from an unsecure network

FIGURE 12.9 Data from a secure network

Antenna Placement

Antenna placement can be crucial in allowing clients to reach the access point. There isn't any one universal solution to this issue, and it depends on the environment in which the access point is placed. As a general rule, the greater the distance the signal must travel, the more it will attenuate, but you can lose a signal quickly in a short space as well if the building materials reflect or absorb the signal. You should try to avoid placing access points near metal (which includes appliances) or near the ground. In the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include *power level controls* that allow you to reduce the amount of output provided.

Real World Scenario

Estimating Signal Strength

One of the most troublesome aspects of working with wireless networks is trying to compute the strength of the signal between the wireless AP and the client(s). It's often joked that a hacker can stand outside a building and tap into your network but a user within the building can't get a strong enough signal to stay on the network.

Think of the signal in terms of any other radio signal—its strength is reduced significantly by cinderblock walls, metal cabinets, and other barriers. The signal can pass through glass windows and thin walls with no difficulty.

When you're laying out a network, it's highly recommended that you install a strength meter on a workstation—many are free to download—and use it to evaluate the intensity of the signal you're receiving. If the signal is weak, you can add additional APs and repeaters to the network, just as you would on a wired network.

A great source for information on RF power values and antenna can be found on the Cisco site at

`http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00800e90fe.shtml`

MAC Filtering

Most APs offer the ability to turn on *MAC filtering*, but it is off by default. The MAC address is the unique identifier that exists for each network card (part of the hexadecimal address identifies the manufacturer, and the other part acts as a serial number). In the default stage, any wireless client that knows the values looked for can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with the users' computers and enters those. When a client attempts to connect, and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise it is forbidden from so doing. On a number of wireless devices, the term *network lock* is used in place of MAC filtering, and the two are synonymous.

The weakness with MAC filtering is that the MAC address is a value that a miscreant could spoof in order to gain entry. By making it look as if their illegitimate host is a legitimate host, they will pass through the filter and be allowed access.

In Exercise 12.1, I'll show you how to change the order of preferred networks in Windows Vista. Preferred networks are limited in Windows 7 and Windows Vista to networks that you have successfully connected to.

EXERCISE 12.1

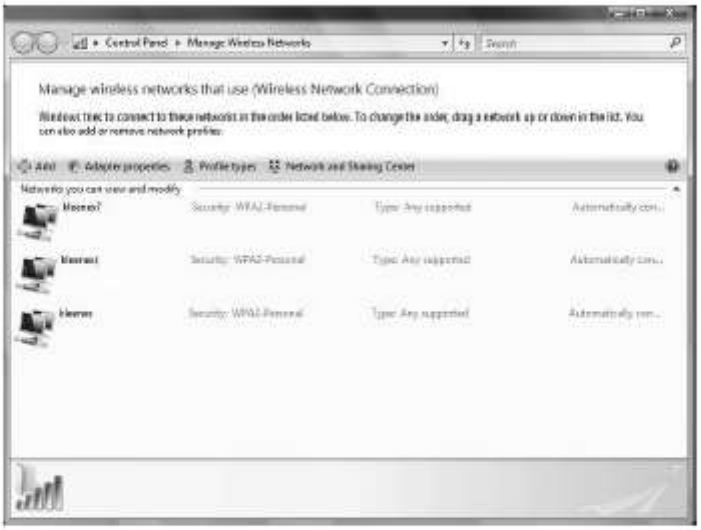
Change the Order of Preferred Networks

Most wireless clients are able to receive signals from, and connect to, more than one wireless network. If one wireless network is not available, the connection will often drop down to the next in this list, and thus it is important to have the wireless networks on the client in the order in which you want them to attempt connection. The following exercise will allow changes to this order:

1. On a Windows Vista client click the Windows button, type **Network and Sharing Center** into the search bar, and press Enter.

EXERCISE 12.1 *(continued)*

2. Choose Manage Wireless Networks.



3. Click any network that appears in the list, and drag it up or down to change the order of the preferred networks.
4. Exit out of Manage Wireless Networks.
5. Exit the Network and Sharing Center.

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) provides a framework for authentication that is often used with wireless networks. Among the five EAP types adopted by the WPA/WPA2 standard are EAP-TLS, EAP-PSK, EAP-MD5, and two that you need to know for the exam: LEAP and PEAP. Figure 12.10 shows that the configuration information on a WLAN card is using EAP-TTLS; this is a form of EAP-TLS that adds tunneling (Extensible Authentication Protocol—Tunneled Transport Layer Security).

FIGURE 12.10 Using EAP-TTLS on a wireless network

By adding the tunneling, TTLS adds one more layer of security against man-in-the-middle attacks or eavesdropping.

Lightweight Extensible Authentication Protocol

Lightweight Extensible Authentication Protocol (LEAP) was created by Cisco as an extension to EAP but is being phased out in favor of PEAP. Because it is a proprietary protocol to Cisco and created only as a quick fix for problems with WEP, it lacks native Windows support.

LEAP requires mutual authentication to improve security but is susceptible to dictionary attacks. It is considered a weak EAP protocol, and Cisco does not currently recommend using it.

An excellent white paper on wireless LAN security from Cisco that discusses LEAP architecture can be found at `http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_white_paper09186a00800b469f_ps4570_Products_White_Paper.html`.

Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) was created by Cisco, RSA, and Microsoft. It replaces LEAP and there is native support for it in Windows (which previously favored EAP-TLS) beginning with Windows XP. There is support for it in all Windows operating systems since then, including Windows Vista and Windows 7.

While many consider PEAP and EAP-TTLS to be similar options, PEAP *is* more secure since it establishes an encrypted channel between the server and the client.

The same Cisco white paper on wireless LAN security discussing LEAP outlines the PEAP authentication process and can be found at `http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_white_paper09186a00800b469f_ps4570_Products_White_Paper.html`.

Wireless Vulnerabilities to Know

Wireless systems are vulnerable to all the different attacks that wired networks are vulnerable to. However, because these protocols use radio frequency signals for *data emanation*, they have an additional weakness: All radio frequency signals can be easily intercepted. To intercept 802.11*x* traffic, all you need is a PC with an appropriate 802.11*x* card installed. Many networks will regularly broadcast their name (known as an *SSID broadcast*) to announce their presence. Simple software on the PC can capture the link traffic in the wireless AP and then process this data in order to decrypt account and password information.

One method of "protecting" the network that is often recommended is to turn off the SSID broadcast. The access point is still there and can still be accessed by those who know of it, but it prevents those who are just scanning from finding it. This should be considered a *very* weak form of security because there are still other ways, albeit a bit more complicated, to discover the presence of the access point besides the SSID broadcast.

In Exercise 12.2, I'll show you how to configure Windows Vista to connect to a network not broadcasting an SSID.

EXERCISE 12.2

Configure a Wireless Connection Not Broadcasting

To configure the client to connect to a network even if the SSID is not broadcasting, follow these steps:

1. On a Windows Vista client, right-click the network icon and choose Connect To A Network.

2. Right-click the network you are connected to and choose Properties.

EXERCISE 12.2 *(continued)*

3. Choose the Connection tab and check the box Connect Even If The Network Is Not Broadcasting.

4. Click OK.
5. Exit from the Connect To A Network dialog box.

An additional aspect of wireless systems is the *site survey*. Site surveys involve listening in on an existing wireless network using commercially available technologies. Doing so allows intelligence, and possibly data capture, to be performed on systems in your wireless network.

The term *site survey* initially meant determining whether a proposed location was free from interference. When used by an attacker, a site survey can determine what types of systems are in use, the protocols used, and other critical information about your network. It's the primary method used to gather data about wireless networks. Virtually all wireless networks are vulnerable to site surveys.

If wireless portals are installed in a building, the signals will frequently radiate past the inside of the building, and they can be detected and decoded outside the building using inexpensive equipment. The term *war driving* refers to driving around town with a laptop looking for APs that can be communicated with. The network card on the laptop is set to promiscuous mode, and it looks for signals coming from anywhere. After intruders gain access, they may steal Internet access or corrupt your data.

Once weaknesses have been discovered in a wireless network, *warchalking* (referenced by CompTIA as two words: "war chalking") can occur. Warchalking involves those who

discover a way into the network leaving signals (often written in chalk) on, or outside, the premise to notify others that the vulnerability is there. The marks can be on the sidewalk, the side of the building, a nearby signpost, and so on and resemble those shown in Figure 12.11. Figure 12.12 shows an example of what would be present for an open node.

FIGURE 12.11 The warchalking symbols

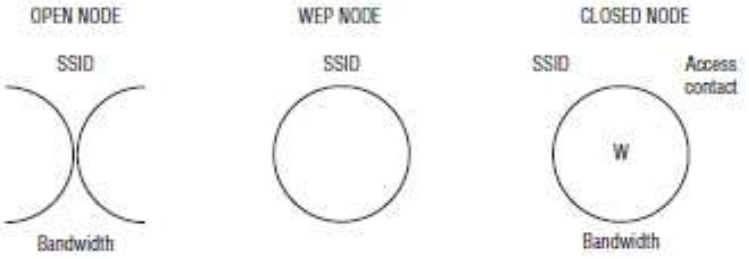


FIGURE 12.12 An example of an open node symbol

Weak encryption was an issue with earlier access points, but most of the newer wireless controllers use special ID numbers (SSID) and must be configured in the network cards to allow communications. However, using ID number configurations doesn't necessarily prevent wireless networks from being monitored, and one particularly mischievous undertaking involves taking advantage of *rogue access points*. Any wireless access point added to your network that has not been authorized is considered a rogue.

The rogue may be added by an attacker, or could have been innocently added by a user wanting to enhance their environment—the problem with the user doing so is that there is a good chance they will not implement the security you would, and this could open the system for a man-in-the-middle attack or *evil twin attack*. An evil twin attack is one in which a rogue wireless access point poses as a legitimate wireless service provider to intercept information users transmit.

Educate and train users about the wireless network and the need to keep it secure, just as you would train and educate them about any other security topic. They may think there is no harm in them joining any wireless network they can find as they travel, such as those

shown in Figure 12.13, but you should question whether the administrators for *Where the party at* really have the best interest of your company data at heart.

FIGURE 12.13 An example of some questionable wireless networks available for users to connect to

Be sure to change the default settings on all wireless devices. Never assume that a wireless connection is secure. The emissions from a wireless portal may be detectable through walls and for several blocks from the portal. Interception is easy to accomplish, given that RF is the medium used for communication. Newer wireless devices offer data security, and you should use it. You can set newer APs and wireless routers to non-broadcast in addition to configuring WPA2 and a higher encryption level.

With the popularity of Bluetooth on the rise, two additional vulnerabilities have been added: *bluejacking* and *bluesnarfing*. Bluejacking is the sending of unsolicited messages (think spam) over the Bluetooth connection. While annoying, it is basically considered harmless. Bluetooth is often used for creating personal area networks (PANs), and most Bluetooth devices come with a factory default PIN that you will want to change to more secure values.

Bluesnarfing is the gaining of unauthorized access through a Bluetooth connection. This access can be gained through a phone, PDA, or any device using Bluetooth. Once access has been gained, the attacker can copy any data in the same way they would with any other unauthorized access.

The Bluetooth standard has addressed weaknesses in the technology, and it continues to get more secure. One of the simplest ways to secure Bluetooth devices is to not set their attribute to Discoverable.

Summary

Wireless systems are becoming increasingly popular and standardized. The most common protocol implemented in wireless systems is WAP. The security layer for WAP is WTLS. WAP is equivalent to TCP/IP for wireless systems.

The standards for wireless systems are developed by the IEEE. The most common standards are 802.11, 802.11a, 802.11b, 802.11i, 802.11g, and 802.11n. These standards use the 2.4GHz or 5GHz frequency spectrum with the exception of 802.11i which is a security standard often referred to as WPA2. Several communications technologies are available to send messages between wireless devices.

Wireless networks are vulnerable to site surveys. Site surveys can be accomplished using a PC and an 802.11*x* card. The term *site survey* is also used in reference to detecting interference in a given area that might prevent 802.11*x* from working.

There are a number of security standards for wireless networking, with WEP (Wired Equivalent Privacy) being the first widely used. It was fraught with errors and replaced in most implementations by WPA (Wi-Fi Protected Access), which used TKIP. This was an intermediate solution that implemented only a portion of the 802.11i standard. The final solution—a full implementation of the 802.11i standard—is WPA2, which uses CCMP.

Vulnerabilities exist because of weaknesses in the protocols. As an example, WEP is vulnerable because of weaknesses in the way the encryption algorithms are employed; the initialization vector (IV) that WEP uses for encryption is 24-bit and IVs are reused with the same key. By examining the repeating result, it is easy for miscreants to crack the WEP secret key, known as using an IV attack.

Mobile devices use either RF signaling or cellular technologies for communication. If the device uses WAP, several levels of security exist: anonymous authentication (anyone can connect), server authentication (the workstation must authenticate against the server), and two-way authentication (both the client and server must authenticate with each other).

Exam Essentials

Know the protocols and components of a wireless system. The backbone of most wireless systems is WAP. WAP can use WEP to provide security in a wireless environment. WTLS is the security layer of WAP. WAP and TCP/IP perform similarly.

Know the hardware used in a wireless network. The wireless access point (AP) sits on the wired network and then acts as the router for the wireless clients. Most of the time, a wireless access point will work with more than one 802.11 standard. Wireless clients, using a wireless NIC card, connect to the access point.

Know the capabilities and limitations of the 802.11*x* network standards. The current standards for wireless protocols are 802.11, 802.11a, 802.11b, and 802.11g. The 802.11n standard is undergoing review and isn't yet a formal standard.

Know the vulnerabilities of wireless networks. The primary method of gaining information about a wireless network is a site survey. Site surveys can be accomplished with a PC and an 802.11 card. Wireless networks are subject to the same attacks as wired networks.

Know the wireless security protocols. The 802.11i standard is often referenced as WPA2. It is an enhancement to earlier standards such as WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access), which were much weaker.

Review Questions

1. Which protocol is mainly used to enable access to the Internet from a mobile phone or PDA?
   - A. WEP
   - B. WTLS
   - C. WAP
   - D. WOP
2. Which protocol operates on 2.4GHz and has a bandwidth of 1 Mbps or 2 Mbps?
   - A. 802.11
   - B. 802.11a
   - C. 802.11b
   - D. 802.11g
3. You're outlining your plans for implementing a wireless network to upper management. Suddenly, a paranoid vice president brings up the question of security. Which protocol was designed to provide security to a wireless network and can be considered equivalent to the security of a wired network?
   - A. WAP
   - B. WTLS
   - C. WPA2
   - D. IR
4. Which of the following is a primary vulnerability of a wireless environment?
   - A. Decryption software
   - B. IP spoofing
   - C. A gap in the WAP
   - D. Site survey
5. Which of the following is synonymous with MAC filtering?
   - A. TKIP
   - B. Network lock
   - C. EAP-TTLS
   - D. MAC secure
6. Which of the following 802.11 standards is often referenced as WPA2?
   - A. 802.11a
   - B. 802.11b
   - C. 802.11i
   - D. 802.11n

7. Which of the following 802.11 standards provides for bandwidths of up to 300 Mbps?
   A. 802.11n
   B. 802.11i
   C. 802.11g
   D. 802.11b
8. An IV attack is usually associated with which of the following wireless protocols?
   A. WEP
   B. WAP
   C. WPA
   D. WPA2
9. Which type of encryption does CCMP use?
   A. EAP
   B. DES
   C. AES
   D. IV
10. Which encryption technology is associated with WPA?
   A. TKIP
   B. CCMP
   C. WEP
   D. LDAP
11. Which of the following is not one of the three transmission technologies used to communicate in the 802.11 standard?
   A. DSSS
   B. FHSS
   C. VITA
   D. OFDM
12. What is the size of the initialization vector (IV) that WEP uses for encryption?
   A. 6-bit
   B. 24-bit
   C. 56-bit
   D. 128-bit
13. Which of the following is a script language WAP-enabled devices can respond to?
   A. WXML
   B. Winsock
   C. WIScript
   D. WMLScript

14. Which of the following authentication levels with WAP requires both ends of the connection to authenticate to confirm validity?
    - A. Relaxed
    - B. Two-way
    - C. Server
    - D. Anonymous
15. Which of the following manages the session information and connection between wireless devices?
    - A. WSP
    - B. WPD
    - C. WPT
    - D. WMD
16. Which of the following provides services similar to TCP and UDP for WAP?
    - A. WTLS
    - B. WDP
    - C. WTP
    - D. WFMD
17. Which of the following authentication levels with WAP allows virtually anyone to connect to the wireless portal?
    - A. Relaxed
    - B. Two-way
    - C. Server
    - D. Anonymous
18. If the interconnection between the WAP server and the Internet isn't encrypted, packets between the devices may be intercepted. What is this vulnerability known as?
    - A. Packet sniffing
    - B. Minding the gap
    - C. Middle man
    - D. Broken promise
19. WAP uses a smaller version of HTML for Internet displays. This is known as:
    - A. DSL
    - B. HSL
    - C. WML
    - D. OFML

20. What is the size of the wrapper TKIP places around the WEP encryption with a key that is based on such things as the MAC address of your machine and the serial number of the packet?

A. 128-bit

B. 64-bit

C. 56-bit

D. 12-bit

Answers to Review Questions

1. C. Wireless Application Protocol (WAP) is an open international standard for applications that use wireless communication.
2. A. 802.11 operates on 2.4GHZ. This standard allows for bandwidths of 1 Mbps or 2 Mbps.
3. C. Wi-Fi Protected Access 2 (WPA2) was intended to provide security that's equivalent to the security on a wired network and implements elements of the 802.11i standard.
4. D. A site survey is the process of monitoring a wireless network using a computer, wireless controller, and analysis software. Site surveys are easily accomplished and hard to detect.
5. B. The term *network lock* is synonymous with MAC filtering.
6. C. The WPA2 standard is also known as 802.11i.
7. A. The 802.11n standard provides for bandwidths of up to 300Mbps.
8. A. An IV attack is usually associated with the WEP wireless protocol.
9. C. CCMP uses 128-bit AES encryption.
10. A. The encryption technology associated with WPA is TKIP.
11. C. The three technologies available for use with the 802.11 standard are DSSS (direct-sequence spread spectrum), FHSS (frequency-hopping spread spectrum), and OFDM (orthogonal frequency division multiplexing). VITA (Volunteer Income Tax Assistance) is not a wireless transmission technology.
12. B. The initialization vector (IV) that WEP uses for encryption is 24-bit.
13. D. WAP-enabled devices can respond to scripts using an environment called WMLScript.
14. B. Two-way authentication requires both ends of the connection to authenticate to confirm validity.
15. A. WSP (Wireless Session Protocol) manages the session information and connection between wireless devices.
16. C. The Wireless Transaction Protocol (WTP) provides services similar to TCP and UDP for WAP.
17. D. Anonymous authentication allows virtually anyone to connect to the wireless portal.
18. A. If the interconnection between the WAP server and the Internet isn't encrypted, packets between the devices may be intercepted and this is known as packet sniffing.
19. C. WAP uses a smaller version of HTML called Wireless Markup Language (WML) for Internet displays.
20. A. TKIP places a 128-bit wrapper around the WEP encryption with a key that is based on such things as the MAC address of your machine and the serial number of the packet.