Capítulo 2 - Introducción a la terminología de seguridad

OBJETIVOS DE CERTIFICACIÓN

2.01 Objetivos de la seguridad de la información

2.02 Descripción de la autenticación y la autorización

2.03 Comprensión de los principios y la terminología de seguridad

2.04 Analizar las funciones y responsabilidades de seguridad

✓ Simulacro de dos minutos

Preguntas y respuestas Autocombado

Si ha revisado los conceptos básicos de redes que necesita saber para el examen de certificación Security+ y para tener éxito como profesional de la seguridad, es hora de sumergirse en algunos conceptos y principios básicos de seguridad. El objetivo de este capítulo es exponerlo a algunos términos y conceptos de seguridad importantes que necesitará saber para el examen, pero también para futuros temas de este libro. Algunos de estos temas, como la autenticación y la autorización, se tratan con mayor detalle en capítulos posteriores; el objetivo aquí es asegurarse de que se sienta cómodo con la terminología de seguridad básica.

OBJETIVO DE CERTIFICACIÓN 2.01

Objetivos de la seguridad de la información

Como profesional de la seguridad, usted trabaja para lograr los objetivos fundamentales de la seguridad de la información. Esos objetivos fundamentales son la confidencialidad, la integridad (integridad de los datos) y la disponibilidad, también conocida como CIA. Esta sección está diseñada para explicarle qué es la CIA y para dar ejemplos de tecnologías populares utilizadas para ayudar a mantener la CIA.

Confidencialidad

Uno de los objetivos de la seguridad de la información es garantizar la confidencialidad de modo que solo las personas autorizadas puedan acceder a la información y puedan leer la información. Se pueden utilizar varias tecnologías, como permisos y cifrado, para mantener la confidencialidad de la información.

Control de acceso/Permisos

La mayoría de los administradores de red protegen la información en la red de la organización mediante la implementación de permisos en los archivos y carpetas. Esto se conoce como crear una *lista de control de acceso (ACL)* en los archivos porque el administrador de red controla quién puede acceder a los archivos. Al establecer permisos en los archivos y permitir que solo un grupo específico de usuarios acceda a los archivos (consulte la Figura 2-1),está ayudando a mantener la confidencialidad.

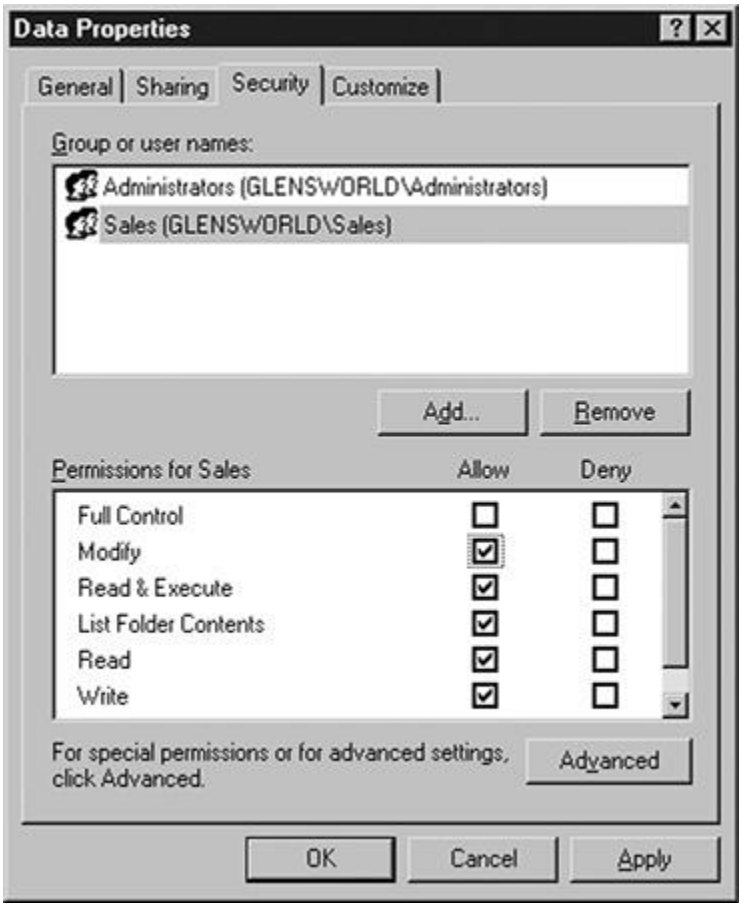


FIGURA 2-1

Control del acceso a los recursos mediante la configuración de permisos

Observe en la figura 2-1 que los permisos de archivo están establecidos para permitir que solo el grupo Ventas y el grupo Administradores tengan acceso al archivo. Si estos grupos son los únicos a los que se les permite acceder al archivo, ha ayudado a mantener la confidencialidad de los datos.

Encriptación

Establecer permisos de archivo en los datos no es suficiente por sí solo para mantener la confidencialidad, ya que la mayoría de las empresas almacenan la información en un servidor y los usuarios tienen que acceder a los datos desde sus equipos cliente a través de la red. Los permisos garantizan que solo las cuentas de usuario adecuadas puedan obtener acceso a los archivos, pero cuando los usuarios descargan esos archivos en sus equipos a través de la red, los permisos de archivo no protegen el contenido del archivo de ser leído mientras los archivos están en tránsito. Aquí es donde encaja el cifrado: el cifrado de la información la coloca en un formato ilegible hasta que una persona autorizada descifra la información, lo que la coloca de nuevo en un formato legible.

Puede cifrar el archivo en dos niveles, mientras el archivo está almacenado y mientras está en tránsito de una ubicación a otra. El beneficio de cifrar el archivo en el almacenamiento es que si los piratas informáticos pueden obtener acceso físico al sistema, normalmente pueden omitir los permisos establecidos por el sistema. Si cifra los datos almacenados y un pirata informático de alguna manera elude los permisos, se habrá asegurado de que los datos sean ilegibles.

Cuando se cifra la información en tránsito, normalmente se cifra el canal de comunicación entre dos sistemas; es decir, todos los datos que corren por el canal de comunicación están encriptados. Al cifrar la información en tránsito, se asegura de que alguien que aprovecha la comunicación no pueda leer la información que ha aprovechado.

Uno de los principales objetivos de la seguridad de la información es mantener la confidencialidad de la información. Puede lograr esto implementando el cifrado de datos y comunicaciones e implementando conceptos de control de acceso como permisos.

Esteganografía

Otra forma de ocultar la información, en un intento de mantenerla confidencial, es mediante el uso de esteganografía. *La esteganografía* es un método para ocultar información en áreas no invisibles de otro archivo. Por ejemplo, puede incrustar un archivo de texto en un archivo gráfico. La información se coloca en el archivo gráfico utilizando un programa y se coloca una contraseña en el archivo. Después de enviar el gráfico al receptor previsto, el receptor previsto usaría la aplicación de esteganografía para leer la información de texto del archivo. Otros ejemplos de esteganografía implican ocultar datos en archivos MP3 y archivos de video.

La esteganografía también es utilizada por personas con motivos maliciosos para transmitir información secreta. Por ejemplo, un grupo internacional de hackers podría usar un sitio web de aspecto normal que contenga imágenes en páginas web para comunicarse entre sí. Los miembros podrían ocultar archivos de texto que detallan su próxima trama en los gráficos,

sabiendo que los otros piratas informáticos del grupo pueden acceder al sitio web, descargar el gráfico y luego usar el programa de esteganografía para extraer el archivo de texto del gráfico.

Integridad

El concepto de integridad de los datos consiste en garantizar que cuando los datos se envían desde una fuente a un destino, la información recibida en el destino no se haya alterado en tránsito. La integridad de los datos también significa que si almacena un archivo en la unidad y lo abre más tarde, puede estar seguro de que los datos no se han alterado mientras están almacenados.

Hash

Para garantizar la integridad de los datos al comunicarse a través de una red, el sistema de envío ejecuta los datos a través de un algoritmo matemático, conocido como *algoritmo hash,* que luego genera una respuesta (conocida como el *valor hash).* Este valor hash se envía con los datos. En el extremo receptor de la transmisión, el sistema de destino ejecuta los datos a través del mismo algoritmo matemático para generar una respuesta (valor hash). Una vez que el sistema de destino tiene su propio valor hash calculado, lo compara con el valor hash enviado con el mensaje; si son los mismos, se supone que los datos no se han alterado. Este proceso se muestra en la Figura 2-2.

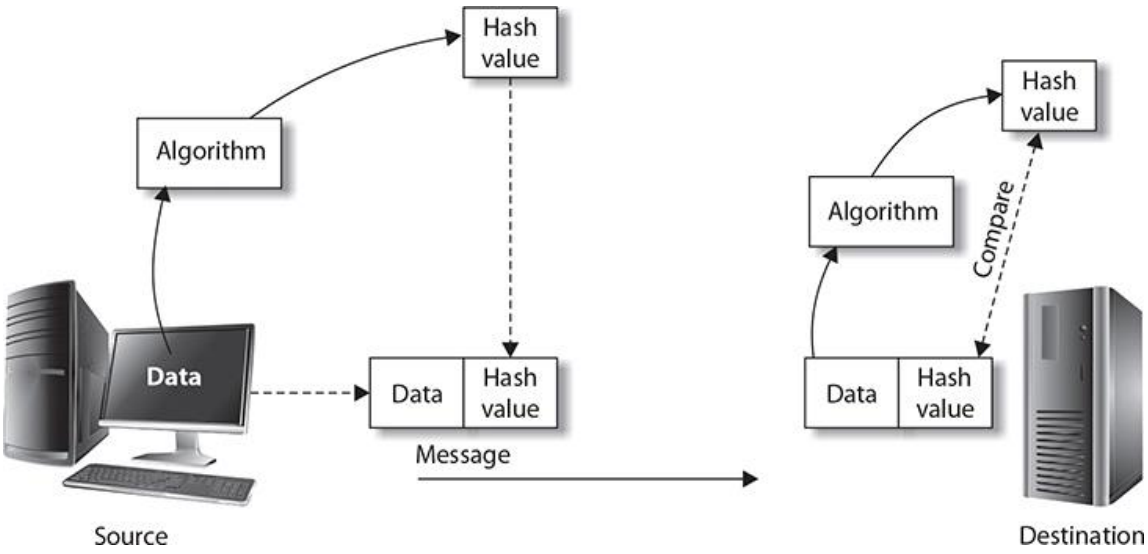


FIGURA 2-2

Garantizar la integridad mediante hash de los datos

La integridad de los datos no se trata solo de la integridad de los datos en tránsito, sino también de los datos almacenados. En entornos altamente seguros, es posible que desee asegurarse de que después de que un usuario almacena un archivo, el archivo no se puede modificar hasta

que el usuario vuelva a abrir el archivo. Para comprobar la integridad del archivo, puede utilizar un programa de integridad de archivos que calcule los valores hash en el archivo cuando se guarda el archivo y, a continuación, compare el valor hash almacenado con el valor hash calculado cuando el archivo se abre de nuevo. Si el archivo ha cambiado desde la última vez que el usuario trabajó con el archivo, los valores hash serán diferentes y se notificará al usuario que el archivo se ha cambiado.

La integridad implica garantizar que los datos que envía son los que se reciben en el otro extremo de la comunicación. El hashing es una tecnología popular utilizada para garantizar la integridad de los datos.

La integridad de los datos se utiliza en muchos escenarios hoy en día; algunos de esos escenarios siguen:

■ **Descarga de archivos** Cuando descarga un programa de Internet, la mayoría de los proveedores le dicen el valor hash del archivo que está descargando para que pueda hacer su propia verificación de integridad en el archivo después de descargarlo. Realizar una comprobación de integridad en el archivo descargado asegurará que el archivo no se haya alterado durante la descarga.

■ **Aplicación de** la ley Cuando los organismos encargados de hacer cumplir la ley realizan una investigación en la computadora de un sospechoso, deben generar un valor hash en los datos antes de siquiera mirarlo para que puedan demostrar más tarde en la corte que no alteraron ni plantaron la información. Si la evidencia entra en cuestión, se comparan los valores hash de los datos antes y después de la investigación; si son los mismos, los datos no se alteraron.

Otro punto a destacar sobre la integridad de los datos es que la implementación de soluciones como los permisos puede ayudar a proteger la integridad de los datos de la información, ya que si controla quién puede modificar los datos, puede protegerlos de cambios no autorizados.

Otros conceptos de integridad

El hashing no es el único concepto de integridad con el que debe estar familiarizado para el examen de certificación Security+; también debe estar familiarizado con los siguientes términos y conceptos de seguridad:

■ **Firma digital** Se crea una firma digital en un mensaje para demostrar la integridad del remitente del mensaje. Debido a que la firma se crea utilizando la clave privada de una persona y solo esa persona tiene acceso a su clave privada, demuestra que el remitente es quien dice ser. Aprenderá más sobre firmas digitales y criptografía en los capítulos 12 y 13.

■ **Certificado digital** Un certificado digital es un archivo electrónico utilizado para transportar claves para cifrar o firmar digitalmente mensajes. Aprenderá más sobre certificados y criptografía en los capítulos 12 y 13.

■ **No repudio** La no repudiación es el concepto de garantizar que alguien no pueda discutir que envió un mensaje o realizó un cambio, lo que aumenta la integridad del sistema. Puede utilizar firmas digitales o auditoría como método para implementar la no auditoría.

Disponibilidad

La disponibilidad, el tercer objetivo fundamental de la seguridad de la información en la tríada de la CIA, es el concepto de garantizar que la información esté disponible cuando el usuario lo desee. Este es un aspecto a menudo pasado por alto de la seguridad de la información.

Puede utilizar una serie de técnicas para garantizar la disponibilidad, todas las cuales se explicarán con más profundidad en el Capítulo 16. Las siguientes son soluciones populares que puede implementar para ayudar a mantener la disponibilidad:

■ **Permisos** La implementación de permisos en un recurso es una forma de ayudar a garantizar la disponibilidad, porque si limita quién puede eliminar los datos, es muy probable que sigan estando disponibles cuando sea necesario.

■ **Copias de seguridad** Asegúrese de realizar copias de seguridad periódicas de la información crítica para que, si los datos se corrompen o no están disponibles, pueda restaurarlos desde la copia de seguridad.

■ **Tolerancia a fallos** Puede implementar soluciones de redundancia de datos para garantizar que si uno de los discos duros falla, las otras unidades tengan una copia de la información. Tener varias unidades trabajando juntas de esta manera se conoce como RAID, o matriz redundante de discos independientes. Con RAID, si una de las unidades falla, las otras unidades proporcionan los datos que faltan.

■ **Clustering** Para garantizar la disponibilidad de servicios como servidores de correo electrónico o bases de datos, puede utilizar una solución de alta disponibilidad como la clustering. La agrupación en clústeres le permite tener varios servidores que actúan como una unidad, de modo que si un servidor falla, otro servidor se hace cargo de la carga de trabajo. Por ejemplo, puede tener su servidor de correo electrónico instalado en ambos servidores *(llamados nodos),*con un servidor que actúa como nodo activo (actualmente en línea) y el otro servidor que actúa como nodo pasivo (no en línea). Cuando el nodo activo falla, el nodo pasivo se convierte en el nodo activo para que los usuarios sigan teniendo acceso al correo electrónico.

■ **Parcheo** Mantener un sistema actualizado mediante la aplicación de Service Packs y revisiones de seguridad se conoce como parcheo. Parchear un sistema ayuda a reducir las vulnerabilidades en el sistema y reduce las posibilidades de ataque.

Una función de la seguridad de la información que a menudo se pasa por alto es garantizar la disponibilidad de datos o servicios. Las técnicas populares para garantizar la disponibilidad son las copias de seguridad de datos y las soluciones de alta disponibilidad, como RAID (matriz redundante de discos independientes) y la agrupación en clústeres.

Responsabilidad

Una tendencia en los últimos años es designar la *A* en la CIA para representar tanto la disponibilidad como la rendición de cuentas (o agregar una *A* para representar la rendición de cuentas, CIAA). La responsabilidad es garantizar que los usuarios sean responsables de sus acciones: si alguien elimina inapropiadamente un archivo, por ejemplo, existe un registro de esa acción para responsabilizarlos.

La responsabilidad se implementa en la organización mediante la implementación de características de auditoría y registro en los sistemas, enrutadores, firewalls y en las aplicaciones. El concepto aquí es que si registra la actividad y puede identificar quién causó que ocurra un determinado evento, puede responsabilizar a esa persona por sus acciones. Los siguientes son algunos métodos populares para implementar la rendición de cuentas dentro de la organización:

■ Archivos de registro La mayoría **de los** servicios de red implementan el registro de forma predeterminada o se pueden configurar para registrar la actividad en los archivos de registro. Asegúrese de habilitar el registro para todos los servicios principales de la red para que, si surge un incidente, pueda revisar los datos registrados.

■ **Archivos de auditoría** La mayoría de los sistemas operativos tienen una función de auditoría de seguridad que le permite revisar los eventos relacionados con la seguridad que ocurren en un sistema. En Windows, este es el registro de seguridad en el Visor de eventos. Asegúrese de revisar los registros de auditoría de seguridad de forma regular.

■ **Cortafuegos y servidores proxy** La mayoría de los cortafuegos y servidores proxy pueden registrar la actividad de los usuarios salientes, como los sitios web que se visitan y las aplicaciones utilizadas para la comunicación saliente. Asegúrese de revisar los registros del firewall y del servidor proxy de forma regular para responsabilizar a los usuarios por sus acciones.

■ **Registro de aplicaciones** Cada vez es más importante registrar la actividad dentro de las aplicaciones. Por ejemplo, si alguien elimina un registro de cliente o una compra del sistema de compras, desea saberlo. Averigüe qué niveles de registro están disponibles en todas sus aplicaciones críticas y haga saber a los usuarios que está registrando actividad. Esto ayudará a mantenerlos responsables de sus acciones dentro del software empresarial. Por ejemplo, Microsoft SQL Server tiene características que permiten a los desarrolladores de bases de datos implementar el registro y la auditoría en la aplicación de base de datos.

El examen Security+ espera que comprenda la CIA y los diferentes métodos de implementación de confidencialidad, integridad y disponibilidad.

EJERCICIO 2-1

Escenarios de la CIA

En este ejercicio, leerá los siguientes escenarios e identificará qué objetivo de la seguridad de la información se está cumpliendo (confidencialidad, integridad, disponibilidad o responsabilidad).

Term	Scenario
_____	A. You have configured auditing on your SQL server so that if a user deletes a customer record, the information is recorded in the audit log.
_____	B. You have configured BitLocker To Go on a USB drive for Bob to be able to store files on the USB drive in an encrypted format.
_____	C. Sue has configured the e-mail server in a server cluster with another server so that if one of the servers fails, the other server can handle the workload.
_____	D. You place the current budget spreadsheet on the company intranet server so that employees can download the file. You publish the hash value of the file on the web site as well.
_____	E. Critical tasks are divided into different jobs, with each person performing one of the different jobs.

OBJETIVO DE CERTIFICACIÓN 2.02

Descripción de la autenticación y la autorización

Una gran parte de la seguridad de su entorno es asegurarse de implementar alguna forma de identificar y verificar a las personas dentro de la organización y luego controlar a qué recursos, sitios web y áreas de la instalación tienen acceso.

Esta sección está diseñada para presentarle los conceptos de autenticación y autorización. Tenga en cuenta que cada uno de estos temas tiene su propio capítulo dedicado a él, pero quiero asegurarme de que tenga una comprensión básica de los conceptos y la terminología de este capítulo.

Identificación y autenticación

La identificación ocurre antes de la autenticación y es el proceso de hacer que los usuarios se identifiquen en el sistema. El método más popular que utilizan las empresas para identificar a los usuarios individuales es dar a cada usuario un nombre de usuario único. Los usuarios escriben su nombre de usuario en el sistema para identificarse.

Después de que el usuario ingresa la información de identificación (el nombre de usuario), el usuario ingresa la contraseña para esa cuenta con fines de autenticación. La información se envía a un sistema de autenticación que se encarga de verificar que el nombre de usuario y la contraseña sean válidos. Si el nombre de usuario y la contraseña son correctos, se concede al usuario acceso al sistema, pero si la información es incorrecta, se muestra un error y se deniega el acceso.

Los usuarios pueden identificarse y autenticarse en el sistema de varias maneras. A continuación se enumeran algunos métodos populares utilizados con fines de identificación y autenticación:

■ **Nombre de usuario** El método más popular para identificar a los usuarios en la red es darles a cada uno un nombre de usuario único. Para que los usuarios se identifiquen, escriben el nombre de usuario en una pantalla de inicio de sesión. Para autenticarse, escriben la contraseña asociada a ese nombre de usuario.

■ **Tarjeta inteligente** Una tarjeta inteligente es del tamaño de una tarjeta de crédito y tiene un microchip que puede contener datos utilizados por un sistema o aplicación (consulte el lado izquierdo de la Figura 2-3). La tarjeta inteligente se puede utilizar para identificar al propietario único de esa tarjeta inteligente específica. Una vez que la tarjeta inteligente se inserta en el sistema, el usuario escribe un PIN asociado con la tarjeta inteligente para autenticarse en el sistema.

FIGURA 2-3

Se puede usar una tarjeta inteligente (izquierda) y un token SecurID (derecha) durante la autenticación.

■ **Token** Un token de seguridad es un pequeño dispositivo que normalmente se usa para identificar a un individuo y se usa en el proceso de autenticación. De los diferentes tipos de tokens, el más popular es un dispositivo que muestra un número aleatorio en él durante 30 a 60 segundos (consulte el lado derecho de la Figura 2-3). El número aleatorio, el nombre de usuario y la contraseña se utilizan para iniciar sesión.

■ **Biometría** La biometría es el concepto de utilizar parte de su ser físico para autenticarse en el sistema. Por ejemplo, puede escanear una huella digital o una retina para autenticarse en un sistema. Los entornos altamente seguros a menudo utilizan sistemas biométricos porque las características físicas no se pueden replicar.

Para el examen, sepa que antes de que se le pueda dar acceso a los recursos (autorización), primero debe identificarse en el sistema. Su información de identificación se verifica en una base de datos de autenticación para verificar que puede obtener acceso al sistema o instalación (esto se conoce como autenticación).

Autorización

Una vez que el usuario ha sido autenticado, se le da acceso a diferentes recursos; esto se conoce como autorización. Tiene muchas maneras de autorizar a las personas para diferentes recursos.

Los siguientes son algunos ejemplos de autorización:

■ **Permisos** Puede autorizar a las personas a acceder a un archivo dándoles permiso para el archivo o dando a un grupo el permiso de la persona que es miembro del archivo. Este es uno de los métodos más populares de autorización.

■ **ACL del router** Otro ejemplo de implementación de la autorización es mediante la configuración de listas de control de acceso (ACL) en un router. Estas ACL determinan si el enrutador puede aceptar cierto tráfico y enrutarlo a una red diferente.

■ **Servidores proxy** Otro ejemplo popular de autorización es permitir o denegar el acceso a diferentes contenidos web en el servidor proxy. El servidor proxy es un servidor en la red por el que pasa todo el tráfico que se dirige a Internet. El servidor proxy puede controlar qué sitios web se pueden visitar o incluso qué tipos de aplicaciones de Internet pueden ser utilizadas por los usuarios internos.

■ **Instalación** Un último ejemplo de autorización es controlar el acceso a diferentes áreas del edificio. Por ejemplo, la tarjeta inteligente de Bob puede darle acceso al área del edificio en el que trabaja, pero la tarjeta no abre puertas a otras áreas del edificio, no está autorizado a acceder a esas áreas.

DENTRO DEL EXAMEN

Diferenciación de autenticación y autorización

El examen de certificación Security+ seguramente probará sus conocimientos sobre la diferencia entre identificación, autenticación y autorización. Aprenderá más sobre estos conceptos a medida que avance en los capítulos, pero ya debe conocer los conceptos básicos en este punto.

Recuerde que la identificación es la forma en que se identifica en el sistema, como proporcionar un nombre de usuario. La verificación de esa identidad se realiza mediante la especificación de una contraseña, que es el proceso de autenticación. Una vez autenticado, puede acceder al sistema.

Una vez que se haya autenticado, el administrador del sistema puede controlar a qué puede acceder en el sistema a través de la autorización. Un ejemplo de autorización es configurar el permiso Modificar en una carpeta para que esté autorizado a realizar cambios en los archivos de la carpeta.

OBJETIVO DE CERTIFICACIÓN 2.03

Comprender los principios y la terminología de seguridad

En esta sección, aprenderá sobre algunos principios de seguridad populares que no solo son importantes para el examen Security+, sino que también son principios importantes que debe practicar al diseñar el programa de seguridad para su organización. Definitivamente vas a ser evaluado en estos principios en el examen, ¡así que prepárate!

Tipos de seguridad

Antes de sumergirnos en algunos de los principios de seguridad comunes, permítame presentarle algunos de los diferentes tipos de seguridad que puede ser necesario implementar dentro de su organización.

Seguridad física

El primer tipo de seguridad con el que debe familiarizarse es la seguridad física. La seguridad física es el concepto de poder controlar quién tiene acceso físico a los activos dentro de la organización. Por ejemplo, la mayoría de las empresas controlan el acceso a sus servidores colocándolos en una sala cerrada con llave conocida como sala de servidores.

La seguridad física también se ocupa de controlar quién puede ingresar a las instalaciones de la organización colocando una cerca alrededor del perímetro de la instalación y tal vez usando guardias en la puerta de entrada. Aprenderá más sobre la seguridad física en el Capítulo 14.

Seguridad de la comunicación

La seguridad de las comunicaciones es un aspecto de la seguridad que a menudo se pasa por alto porque las empresas parecen centrarse mucho en la seguridad física y también en la configuración de permisos en archivos y carpetas. Establecer permisos en archivos y carpetas ayudará a proteger el activo solo a medida que se almacena en el servidor: ¿qué pasa cuando alguien accede al archivo desde toda la red? Si un usuario que tiene permiso para el archivo accede a él desde toda la red, el archivo se descarga en el equipo cliente. Mientras el archivo se descarga en el equipo cliente, es posible que las partes que no son de confianza aprovechen esa comunicación y vean la información. La seguridad de la comunicación se ocupa de proteger la información que viaja entre el origen y el destino mediante el cifrado de la comunicación.

Seguridad Informática

La seguridad informática es uno de los tipos de seguridad más populares: se ocupa de proteger los sistemas informáticos mediante la implementación de una serie de mejores prácticas, como la autenticación, el control de acceso, la redundancia de datos, la protección contra malware y las técnicas de endurecimiento del sistema. El punto a entender acerca de la seguridad

informática es que usted está asegurando los sistemas, pero no la comunicación entre los sistemas.

Seguridad de red

La seguridad de la red es otro tipo popular de seguridad y se ocupa de proteger la red, no un sistema en particular. La seguridad de la red abarca cosas como controlar quién obtiene acceso a la red (seguridad del conmutador) y qué tipo de tráfico puede ingresar a la red (firewalls). Esto se complementa con el monitoreo del tráfico de red en busca de actividad sospechosa (un sistema de detección de intrusiones).

Ahora que comprende los diferentes tipos de seguridad de red, echemos un vistazo a algunos de los principios de seguridad importantes con los que debe estar familiarizado para el examen de certificación Security +.

Privilegios mínimos, separación de funciones y rotación de funciones

El primer principio de seguridad que siempre debe seguir al dar a los usuarios y administradores de red acceso a recursos como sistemas o archivos es el concepto de privilegios mínimos. *El privilegio mínimo* significa que se otorga a un usuario solo el nivel mínimo de permisos necesarios para realizar sus tareas o tareas. No desea conceder más permisos de los necesarios porque entonces el usuario o administrador puede hacer más de lo que se espera con el recurso. Por ejemplo, si Bob es responsable de hacer las copias de seguridad de un servidor Windows, no desea colocarlo en el grupo Administradores porque tendría la capacidad de hacer más que copias de seguridad: podría realizar cualquier cambio en el sistema que desee. En este ejemplo, desea colocarlo en el grupo Operador de copia de seguridad para que su ámbito se limite a realizar copias de seguridad.

Otro ejemplo involucra permisos de archivo. Si un usuario solo necesita poder leer el contenido de un archivo, asegúrese de darle solo el permiso de lectura y no más, porque de lo contrario podría eliminar accidentalmente el contenido del archivo. Si esto sucediera, ¿quién crees que tendría la culpa: la persona que eliminó el contenido o la persona que le dio el privilegio de eliminar el contenido?

Para el examen, sepa que el término *colusión* significa múltiples personas involucradas en una tarea que se reúnen y participan en actividades fraudulentas.

Separación de funciones

Otro principio importante a practicar dentro de la organización es la separación de deberes. *La separación de tareas* significa que se asegura de que todas las tareas críticas se divida en diferentes procesos y que cada proceso sea realizado por un empleado diferente. Por ejemplo, en la mayoría de las empresas, la persona que escribe el cheque para pagar una compra es diferente de la persona que firma el cheque. Por lo general, la persona que escribe el cheque es alguien en el departamento de contabilidad, pero el cheque generalmente está firmado por el director financiero (CFO) de la empresa.

Un ejemplo centrado en la tecnología de la implementación del concepto de separación de funciones es garantizar que cuando una empresa decide hacer una evaluación de seguridad de red, la evaluación sea realizada por un profesional de seguridad independiente y no por el administrador de red de la empresa.

El concepto de separación de deberes se utiliza para mantener a todos honestos y para prevenir actividades fraudulentas dentro de la organización. Tenga en cuenta que la separación de deberes no lo protegerá de la *colusión,* que es el término utilizado para describir cuando las partes conspiran juntas para cometer un acto fraudulento; por ejemplo, la persona que escribe el cheque y la persona que firma el cheque deciden comenzar a escribir cheques para su propio negocio conjunto.

Rotación de funciones

Otro principio de seguridad importante que se relaciona con el personal y las operaciones comerciales diarias es el concepto de rotación de tareas. *La rotación de tareas* es el principio de rotar a varios empleados a través de diferentes roles de trabajo. Por ejemplo, tiene un equipo de administradores de red, y este mes Bob se encargará de la administración de cuentas, pero el próximo mes Sue asumirá ese deber, y Bob asumirá el rol de trabajo que Tenía Sue.

Para el examen, asegúrese de conocer la diferencia entre la separación de deberes y la rotación de deberes.

La rotación de tareas ofrece múltiples beneficios. En primer lugar, es una forma de garantizar la responsabilidad por las acciones de los empleados. Si Bob ha estado haciendo un mal uso intencional o accidental de sus privilegios, entonces Sue lo notará al mes siguiente y lo informará. El otro beneficio de la rotación de tareas es que la organización no depende de que una persona sea la única persona capaz de desempeñar un puesto de trabajo. Al rotar a varios empleados a través de diferentes roles, la organización tiene cierta redundancia en los conjuntos de habilidades en caso de que un empleado se enferme, se vaya de licencia o renuncie.

Concepto de necesidad de saber

Más adelante en este libro, aprenderá más sobre la autenticación y el control de acceso, pero uno de los principios de seguridad que quería introducir en este capítulo de terminología antes de llegar a esos capítulos es el concepto de necesidad de *saber,* lo que significa que les da a los empleados acceso solo a la información que necesitan conocer. Por ejemplo, en lugar de dar a todos los administradores acceso a los datos contables, desea asegurarse de que solo el administrador de contabilidad tenga acceso a los datos contables. No le da al gerente de marketing acceso a los datos contables porque el gerente de marketing no necesita este acceso.

Otro ejemplo de implementación del concepto de necesidad de saber se encuentra en entornos militares. El hecho de que a un comandante se le haya dado la autorización de alto secreto no significa que deba poder ver todos los datos de alto secreto en la organización. Por ejemplo, si el comandante no está involucrado en una determinada operación, no necesita saber la información que se presenta al personal involucrado en esa operación.

Seguridad en capas y diversidad de defensa

Otros dos principios de seguridad muy importantes que deben seguirse para ayudar a crear un entorno más seguro son los conceptos de adoptar un enfoque de seguridad en capas y la diversidad de defensa. *La seguridad en capas* es el concepto de no poner todos los huevos en una canasta confiando en un tipo de solución de seguridad para crear un entorno seguro. Por ejemplo, aunque los firewalls son una parte crítica de la seguridad para cualquier organización, si alguien trae una unidad flash que está infectada con un virus a la oficina, el firewall no ayudará a proteger los sistemas. Adoptar un enfoque en capas de la seguridad significa que confiará en muchos tipos diferentes de controles de seguridad, como la autenticación, la protección antivirus, los sistemas de parches y los firewalls. Adoptar un enfoque en capas para la seguridad también se conoce como "defensa en*profundidad".*

La diversidad de defensa es el concepto de que debe utilizar diferentes productos para aumentar el nivel de seguridad en su entorno. Por ejemplo, al diseñar una estrategia de firewall, lo más probable es que tenga varias capas de firewalls, y es importante no usar el mismo producto de firewall en cada capa. Si el hacker descubre cómo hackear el primer firewall y usted está utilizando el mismo producto de firewall en otra parte de la red, el hacker usará la misma técnica para eludir esos firewalls. Si utiliza diferentes productos proporcionados por diferentes fabricantes, el método utilizado para piratear el primer firewall no necesariamente funcionará en el segundo firewall. El concepto aquí es que aunque todos los productos tienen vulnerabilidades, las vulnerabilidades son diferentes para cada uno de los diferentes productos, y el hacker tendrá que trabajar más duro para superar cada producto diferente.

Otro ejemplo de diversidad de defensa es que cuando compra software antivirus para su servidor antispam, su servidor de correo electrónico y sus sistemas de escritorio, asegúrese de usar software antivirus de diferentes proveedores. El propósito de esto es que si el virus pasa

por uno de los productos antivirus, uno de los otros productos antivirus lo atrapará, con suerte. He oído hablar de casos en los que salió un exploit de día cero que fue pasado por alto por el analizador antivirus externo que se ejecuta en el servidor de correo electrónico, pero fue capturado por el software antivirus que se ejecuta en el cliente cuando el archivo adjunto llegó al cliente de correo electrónico. Instancias como esta le ayudan a justificar el costo de ejecutar software antivirus en diferentes capas de la red.

Due Care y Due Diligence

Otros principios importantes de seguridad son los conceptos de debido cuidado y diligencia debida, que tienen la intención de garantizar que la organización esté tomando medidas para hacer lo correcto para proteger a sus empleados y activos. *El debido cuidado* es el concepto de hacer lo correcto. Cuando se trata de seguridad, el debido cuidado consiste en implementar los controles de seguridad correctos para garantizar la protección de los activos de la organización. Los ejemplos incluyen la creación de la política de seguridad, la realización de copias de seguridad periódicas y la realización de análisis de virus regulares. La clave a tener en cuenta con el debido cuidado es que está implementando una acción. *La diligencia debida,* por otro lado, se trata de identificar su riesgo para que sepa qué controles de seguridad implementar (el debido cuidado). La diligencia debida implica realizar evaluaciones periódicas y analizar los resultados de la evaluación para identificar problemas de seguridad en el entorno.

Vulnerabilidad y exploit

Dos términos muy importantes que los profesionales de la seguridad lanzan con bastante frecuencia son vulnerabilidad y explotación. Una *vulnerabilidad* es una debilidad en una pieza de software o hardware que fue creada por el fabricante por accidente. Los hackers pasan bastante tiempo evaluando nuevo software y hardware para tratar de localizar vulnerabilidades. Una vez que los hackers encuentran una debilidad, trabajan en una forma *de explotar* la debilidad y comprometer la seguridad del sistema.

Razones de las vulnerabilidades

El examen Security+ pondrá a prueba sus conocimientos sobre las vulnerabilidades y por qué existen. Hay una serie de razones por las que hay tantas vulnerabilidades hoy en día:

■ **Sistemas al final de su vida útil** Un sistema al final de su vida útil (EOL) es un sistema que ha llegado al final de su utilidad (o rentabilidad) desde el punto de vista de un proveedor. Los sistemas EOL generalmente se conocen como sistemas heredados y pueden ser necesarios dentro de una empresa porque ejecutan una pieza antigua de software que aún no se ha reemplazado. Un sistema EOL presenta un riesgo de seguridad para su empresa porque el proveedor del sistema deja de admitirlo cuando alcanza su fecha de EOL. Por ejemplo, un proveedor no creará parches para ninguna vulnerabilidad nueva que se encuentre en el software que haya llegado a EOL, lo que hace que el sistema sea un gran riesgo de seguridad para la empresa que lo usa.

■ **Sistemas embebidos** Un sistema embebido es un pequeño sistema informático que contiene hardware mínimo, como un procesador, una placa de circuito y memoria, y generalmente una versión reducida de un sistema operativo, y está integrado dentro de un dispositivo o sistema más grande para realizar funciones específicas. Debido a que los dispositivos de hardware ejecutan sistemas integrados con software, son vulnerables a los ataques, al igual que un sistema informático normal si el software en ejecución tiene vulnerabilidades. Los sistemas integrados a menudo se pasan por alto desde el punto de vista de la seguridad, por lo que se debe hacer un esfuerzo adicional para localizar los sistemas integrados y evaluar las vulnerabilidades que puedan existir.

■ **Falta de soporte del proveedor** Una de las principales razones de las vulnerabilidades es la falta de soporte del proveedor. Todo el software tiene vulnerabilidades, y una vez que se ha encontrado una vulnerabilidad, el proveedor generalmente crea una solución para ella. Si está utilizando un producto que el proveedor ya no admite, eso significa que el proveedor ya no está creando correcciones para las vulnerabilidades que surjan.

Tipos de Vulnerabilidades

Existen innumerables vulnerabilidades diferentes en los dispositivos de software y hardware de hoy en día. Muchas de las vulnerabilidades existen debido a errores de programación o mala configuración de sistemas y dispositivos. El examen de certificación Security+ espera que esté familiarizado con estos tipos de vulnerabilidades:

■ **Uso de inteligencia de código abierto** La inteligencia de código abierto (OSINT) es información que está disponible en fuentes públicas como periódicos, revistas, televisión e Internet. Con la cantidad de información que hay en Internet hoy en día, es muy fácil aprender de las vulnerabilidades en un producto.

■ Manejo **inadecuado de entradas** El manejo de entradas es otro trabajo para los programadores de software. Cada vez que se pasan datos a una aplicación, se supone que el programador debe validar esos datos y asegurarse de que sean apropiados para la tarea. Si los datos no son válidos, se muestra un error al usuario en lugar de procesar la información. Si el programador no valida la entrada, los hackers pueden inyectar datos maliciosos en la aplicación para controlar el software de una manera que no se desea.

■ **Configuración incorrecta/configuración débil** La mayoría de las vulnerabilidades existen porque el software o el sistema operativo se han configurado erróneamente y se han colocado en un estado no seguro.

■ **Configuración predeterminada** Al instalar software o sistemas, asegúrese siempre de cambiar la configuración predeterminada. Los hackers conocen las configuraciones predeterminadas de los productos y aprenden a explotar los sistemas basados en las configuraciones predeterminadas. Debe cambiar los valores predeterminados para que los piratas informáticos sean más propensos a darse por vencidos y buscar objetivos más fáciles.

Hay una serie de otras razones por las que los sistemas son vulnerables, como aprenderá progresando a través de los capítulos restantes de este libro.

Actores de amenazas

Los actores de amenazas son individuos que podrían representar un riesgo para la seguridad de sus activos. Esos actores podrían ser hackers, pero también hay otras formas de actores de amenazas a tener en cuenta. Considero que un *hacker* es alguien con el conocimiento para comprometer un sistema, red o instalación. El tipo de hacker depende de la intención del hacker:

■ **Hacker autorizado** También conocido como hacker de sombrero blanco, un hacker autorizado aprende cómo comprometer la seguridad del sistema con fines defensivos, lo que significa que lo están haciendo para aprender mejor cómo proteger el sistema o la red. A un hacker de sombrero blanco se le ha dado autorización para hackear sistemas para ayudar a mejorar la seguridad de esos sistemas.

■ **Hacker no autorizado** También conocido como hacker de sombrero negro, un hacker no autorizado compromete sistemas o redes por razones maliciosas, ya sea por razones financieras, políticas, derechos de fanfarronear o simplemente para causar estragos. Un hacker de sombrero negro no ha recibido autorización para hackear los sistemas.

■ **Hacker semiautor autorizado** También conocido como hacker de sombrero gris, un hacker semiautor autorizado es una persona que piratea sistemas por razones no malsicias (generalmente para ayudar a proteger los sistemas), pero no estaba autorizado a hacerlo.

Tipos de actores

No son solo los hackers contra los que tienes que proteger tus sistemas. Hay muchos tipos de personas, conocidas como actores, que debe conocer y proteger los activos de su organización. La siguiente es una lista de tipos comunes de actores:

■ **Script kiddies** Un script kiddie no tiene mucha educación sobre cómo funciona un ataque, pero es capaz de ejecutar uno descargando un programa, o script, de Internet y usándolo para realizar el ataque. Una vez más, el niño del guión no entiende los detalles del ataque; solo saben que cuando ejecutan el script o programa, les da acceso a un sistema.

■ **Hacktivistas Los** hacktivistas son personas que hackean por principio o por una causa. La causa podría ser creencias políticas, problemas ambientales o apoyo a algo o alguien que necesita ayuda. El bien publicitado grupo Anonymous es un ejemplo de un grupo hacktivista.

■ **Agentes estatales** *Los agentes estatales* son personas que actúan en nombre de su gobierno y se rigen por las regulaciones de ese gobierno.

■ **Amenazas persistentes avanzadas (APT)** *Las amenazas persistentes avanzadas (APT)* son individuos o grupos que realizan ataques altamente completos y bien planificados que les dan acceso a largo plazo a los sistemas de destino. Se necesita acceso a largo plazo a un sistema para que el atacante pueda recopilar información confidencial durante un largo período de tiempo. Para el examen, recuerde que un APT implica un ataque sofisticado y bien organizado que le da al atacante acceso al sistema durante un largo período de tiempo.

■ **Amenazas internas** Un punto muy importante a recordar es que necesita proteger sus activos de las personas dentro de su organización tanto como necesita protegerlos de personas fuera de la organización. ¡Una empresa que se enfoca en tener un firewall para protegerse contra los piratas informáticos en Internet y se olvida por completo de proteger los activos de personas internas o empleados, seguramente tendrá incidentes de seguridad!

■ **Competidores** Los competidores podrían usar hackers para explotar los sistemas de su empresa para descubrir secretos sobre nuevos productos y servicios en los que su empresa está trabajando. También podrían usar hackers para explotar sus sistemas con el fin de causar interrupciones en sus servicios para que sus clientes busquen negocios en otro lugar, es decir, el competidor detrás del exploit.

■ **Sindicatos criminales** Un sindicato criminal es un actor de amenazas que está estrechamente relacionado con el crimen organizado o organizaciones del hampa como la mafia o está afiliado a gángsters.

■ **Shadow IT** Shadow IT es el término utilizado para describir a las personas que implementan sistemas o soluciones de TI sin el conocimiento y el permiso del departamento de TI. Por ejemplo, el departamento de contabilidad puede decidir conectar un enrutador doméstico inalámbrico a la red para que puedan llevar sus computadoras portátiles a diferentes áreas del edificio y aún así tener acceso a la red. Esto presenta un gran riesgo para la compañía porque el enrutador inalámbrico es un dispositivo no autorizado y no se ha implementado siguiendo la política de seguridad de la compañía.

Para el examen, conozca los diferentes tipos de actores que potencialmente pueden ser un riesgo de seguridad para su organización. Asegúrese de centrarse en conocer APT, TI en la sombra, actores estatales, hacktivistas y niños de guión.

Atributos de los actores

Tiene una serie de atributos diferentes a considerar al evaluar el potencial de amenaza de varios actores. Los siguientes son algunos atributos comunes a considerar al evaluar a los actores de amenazas:

■ Los actores **internos/externos** se clasifican típicamente como actores internos o actores externos. Un actor interno podría ser un empleado descontento que quiere tomar represalias por no obtener un aumento salarial o un ascenso. Un actor externo es alguien fuera de la organización que tiene la intención de piratear la red de la organización.

■ **nivel de sofisticación/capacidad** Muchos actores de amenazas tienen un alto nivel de conocimientos técnicos o habilidades sociales; sin embargo, el nivel de sofisticación dependerá del actor. Por ejemplo, un script kiddie generalmente tiene un conocimiento técnico mínimo, pero los atacantes criminales altamente sofisticados generalmente tienen el conocimiento técnico para organizar y ejecutar ataques complejos.

■ **Recursos/financiación** Los actores que se convierten en hackers tienen diferentes niveles de recursos y financiación disponibles para ellos. Por ejemplo, mientras que un niño con guión podría ser un adolescente con recursos bastante limitados en el sótano de sus padres usando una computadora portátil suministrada por la escuela, un hacker patrocinado por el estado puede tener recursos ilimitados, incluido el hardware informático de última generación y herramientas de software sofisticadas.

■ **Intención/motivación** Muchas personas que hackean o realizan acciones maliciosas tienen alguna razón para hacerlo. La motivación podría ser financiera, política, venganza o incluso presumir de derechos.

Vectores de amenaza

Vector de amenaza es el término utilizado para describir los medios que un atacante utiliza para comprometer un sistema. Hay una serie de vectores de amenaza diferentes, como credenciales comprometidas, configuración incorrecta y cifrado deficiente. Los siguientes son vectores de amenaza con los que el examen de certificación de Security+ espera que esté familiarizado:

■ **Acceso directo** El atacante puede tener acceso directo al sistema, lo que le permite explotarlo directamente a través de vulnerabilidades en el sistema.

■ **Inalámbrico** El atacante puede explotar el sistema a través de una red inalámbrica vulnerable o un dispositivo inalámbrico. Esto puede incluir una red inalámbrica 802.11 o tecnología inalámbrica como Bluetooth.

■ **Correo electrónico** El atacante puede atacar un sistema a través de la ingeniería social a través de un mensaje de correo electrónico, como un correo electrónico de phishing que engaña al usuario para que haga clic en un enlace que le da al hacker acceso al sistema.

■ **Cadena de suministro** La cadena de suministro es otro método que los hackers pueden utilizar para comprometer la seguridad de su organización al piratear a los proveedores que le suministran bienes para obtener acceso a sus datos. En algunos casos, su empresa podría tener conexiones de red de empresa a empresa con sus proveedores, lo que podría actuar como una

puerta de enlace a su red si el pirata informático ataca a un proveedor. Alternativamente, si un proveedor le proporciona componentes para su equipo, puede ser más fácil piratear a ese proveedor para obtener exploits en sus productos o en su red.

■ **Redes sociales** Los vectores de ataque de las redes sociales pueden incluir hacerse amigo de una víctima en las redes sociales para que el atacante pueda obtener información perspicaz sobre la víctima prevista y luego enviar un mensaje a la víctima con un enlace que comprometa la seguridad.

■ **Medios extraíbles** Los medios extraíbles, como una unidad flash, podrían ser un vector de ataque, donde el atacante coloca un virus en la unidad USB que se replica en el sistema de la víctima una vez que está conectado a la unidad USB del sistema.

■ **Nube** El entorno de la nube podría ser el método que el hacker utiliza para comprometer su entorno. Su enfoque de seguridad puede ser más estricto para su red que para las soluciones en la nube que está comprando. Algunas soluciones en la nube tendrán una conexión directa de estilo VPN entre la red en la nube y su red local. En este caso, los servidores en la nube deben estar tan protegidos como los sistemas locales para ayudar a evitar que una parte de la seguridad del entorno en la nube permita el acceso a la red local.

Fuentes de inteligencia de amenazas

Hay una serie de recursos disponibles para determinar las amenazas que pueden existir contra una empresa y los activos de la empresa. Por ejemplo, podría utilizar un analizador de vulnerabilidades que utilice una base de datos de vulnerabilidades para obtener una lista de posibles vulnerabilidades para diferentes programas que se encuentran en la red. O bien, un atacante podría usar herramientas de inteligencia de código abierto (OSINT) para obtener información sobre la empresa, como nombres de contacto y direcciones de correo electrónico, que se pueden usar en un ataque de phishing. Las fuentes de inteligencia de amenazas pueden ayudar a una empresa a determinar si es probable que sea vulnerable a los ataques cibernéticos.

Las siguientes son las fuentes de inteligencia de amenazas que los hackers o los probadores de seguridad pueden usar para ayudar a descubrir amenazas a una organización:

■ **Inteligencia de código abierto (OSINT)** Las herramientas de inteligencia de código abierto (OSINT) son de uso gratuito y se utilizan para automatizar la recopilación de información en línea sobre una empresa. Estas herramientas se pueden utilizar para descubrir los sistemas en la red, la información de contacto de los empleados e incluso los dispositivos IoT conectados a Internet. Herramientas como theHarvester y Recon-ng se pueden utilizar para descubrir nombres de contacto, direcciones de correo electrónico e información de direcciones IP de una empresa. Shodan es un motor de búsqueda utilizado para descubrir servidores o dispositivos IoT conectados a Internet para una empresa en particular.

■ **Cerrado/propietario** Las herramientas cerradas o propietarias son herramientas comerciales que tendría que comprar para poder utilizarlas como fuentes de inteligencia de amenazas. Estas herramientas generalmente recopilan y muestran la misma información que las herramientas OSINT, pero tienen un costo para la empresa por su uso.

■ **Bases de datos de** vulnerabilidades Una base de datos de vulnerabilidades es un sitio que puede visitar que le permite buscar vulnerabilidades de un producto en particular. La base de datos de vulnerabilidades informa cada una de las vulnerabilidades y le da una calificación de riesgo bajo, medio o alto. El uso de un analizador de vulnerabilidades puede automatizar la investigación sobre las vulnerabilidades que existen en su entorno.

■ **Centros de intercambio de información públicos/privados** Los centros de intercambio de información suelen ser sitios web utilizados para compartir información sobre amenazas comunes a las organizaciones. Un centro de intercambio de información puede ser de naturaleza pública, lo que significa que cualquier persona tiene acceso a la información, o podría ser privado para su organización.

■ **Dark web** La dark web es una parte de Internet que permite a las personas llevar a cabo sus negocios de forma anónima. Los participantes en la web oscura suelen utilizar tecnologías como Tor para permanecer en el anonimato y ocultar su ubicación.

■ **Indicadores de compromiso (IoCs)** Los indicadores de compromiso (IoCs) son elementos que se encuentran en un sistema que indican que ha habido una violación de seguridad. Las empresas pueden usar información de archivos de registro, archivos en un sistema e incluso métricas en tiempo real para recopilar información sobre una amenaza de seguridad que ocurrió.

■ **Intercambio automatizado de indicadores (AIS)** La Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) ha creado el Intercambio Automatizado de Indicadores (AIS), que permite compartir información de amenazas en tiempo real entre la comunidad CISA para ayudar a prevenir ataques cibernéticos. La información sobre amenazas cibernéticas se comparte entre los sistemas al colocarse en un formato de eXpression de información de amenazas estructuradas (STIX) que luego se puede comunicar a los sistemas que ejecutan el software cliente Trusted Automated eXchange of Intelligence Information (TAXII).

■ **Análisis predictivo** El análisis predictivo es una característica de muchas herramientas de gestión de amenazas que permite al software predecir y determinar los pasos futuros involucrados en una amenaza y activar medidas de protección con anticipación.

■ **Mapas de** amenazas Un mapa de amenazas, también conocido como mapa de ataque, muestra líneas que indican la fuente del ataque y el objetivo del ataque en tiempo real. Para ver un ejemplo de un mapa de amenazas, consulte https://threatmap.checkpoint.com.

■ **Repositorios de archivos/códigos** Los repositorios de archivos o códigos son sitios web que contienen una lista de exploits (amenazas) comunes contra productos y, por lo general, publican el código o un archivo compilado que puede usar para probar el exploit.

Para el examen, conozca las diferentes fuentes de inteligencia de amenazas con el enfoque en mapas de amenazas, OSINT y bases de datos de vulnerabilidades.

Fuentes de investigación

El desafío con la seguridad es mantenerse actualizado sobre los tipos de amenazas y vulnerabilidades que existen para los diferentes tipos de sistemas y activos que tiene su organización. ¡La investigación continua es la clave! Puede utilizar una serie de recursos para mantenerse al día sobre las amenazas y vulnerabilidades que pueden afectar a su empresa:

■ **Sitios web de proveedores** Supervise el sitio web de la empresa que crea los productos que su empresa está utilizando. Por ejemplo, si utiliza enrutadores y conmutadores Cisco, asegúrese de vigilar de cerca el sitio de Cisco para obtener información sobre actualizaciones y avisos de seguridad.

■ **Feeds de vulnerabilidades** Un feed de vulnerabilidades es un feed de noticias proporcionado de forma continua con información actualizada sobre las vulnerabilidades actuales encontradas en diferentes productos.

■ **Conferencias** Puede asistir a conferencias de seguridad que discuten las tendencias actuales con respecto a las amenazas y vulnerabilidades.

■ **Revistas académicas** Puede suscribirse a revistas mensuales o anuales que brindan información detallada sobre los productos que utiliza.

■ **Las solicitudes de comentarios (RFC) las** RFC son normas publicadas y normas propuestas para las tecnologías y protocolos de Internet. Puede leer los documentos RFC para comprender mejor los protocolos o tecnologías de subrayado utilizados por el software y el hardware.

■ **Grupos de la industria local** Puede verificar si hay algún grupo de discusión local en su área que discuta las amenazas comunes a los productos.

■ **Redes sociales** Verifique si hay grupos de redes sociales a los que pueda unirse que compartan información sobre amenazas comunes.

■ **Feeds de** amenazas Un feed de amenazas es similar a un feed de vulnerabilidades, pero proporciona información sobre las diferentes amenazas que tienen tendencias en la industria.

■ **Tácticas, técnicas y procedimientos del adversario (TTP)** Las tácticas, técnicas y procedimientos (TTP) son una descripción de los comportamientos de un actor de amenazas. Una táctica es una descripción de alto nivel de una acción que toma un actor de amenazas. Una técnica es una descripción más detallada de esa táctica, y un procedimiento proporciona detalles paso a paso sobre cómo el actor de la amenaza logra el comportamiento.

OBJETIVO DE CERTIFICACIÓN 2.04

Analizar los roles y responsabilidades de seguridad

La seguridad es una preocupación para todos en la organización, y cada persona desempeñará un papel diferente dentro de la historia de seguridad. Es importante identificar los diferentes roles que las personas asumirán dentro de una organización, como propietario de datos, custodio, usuario y oficial de seguridad.

Propietario del sistema y propietario de los datos

Un término importante para conocer cuando se trata de seguridad de la información es *propietario.* El propietario, ya sea el propietario del sistema o el propietario de los datos, es la persona que decide qué tan valioso es el activo y qué tipos de controles de seguridad deben establecerse para proteger el activo. El propietario también decide la sensibilidad de la información, como el alto secreto cuando se trata de sistemas de clasificación.

El propietario del activo es una gerencia de nivel superior y tiene la responsabilidad final de asegurar el activo y la seguridad dentro de la organización.

Controlador de datos y procesador de datos

En Europa, el Reglamento General de Protección de Datos (RGPD) rige la protección y privacidad de los datos personales. Dentro del GDPR están los controladores de datos y los procesadores de datos. Un *controlador de datos* es una entidad que determina cómo y por qué se procesan los datos personales. El *procesador de datos* es la entidad que realmente realiza el procesamiento de los datos personales, según las pautas establecidas por el controlador de datos.

Administrador del sistema

El administrador del sistema es la persona responsable de la configuración de un sistema o red. El administrador del sistema recibe los objetivos de configuración de los diseñadores o los profesionales de seguridad dentro de la organización y configura los sistemas de manera que cumplan esos objetivos.

Es importante que el profesional de seguridad sea alguien que no sea el administrador del sistema para que el profesional de seguridad pueda auditar las tareas de configuración del administrador del sistema para asegurarse de que la configuración deja un sistema en un estado seguro.

Usuario

Un usuario es cualquier persona que accede y utiliza los recursos dentro de la organización. Un usuario se ve afectado por los controles de seguridad determinados por el propietario y puestos en marcha por el administrador/custodio (consulte "Roles y responsabilidades de datos").

Usuario privilegiado

Un usuario privilegiado es aquel al que se le han otorgado privilegios adicionales para realizar tareas administrativas. Es importante que limite la cantidad de usuarios que son usuarios privilegiados, por varias razones. Por ejemplo, un usuario privilegiado podría cometer un error al usar el sistema, y debido a que tiene privilegios adicionales, podría eliminar accidentalmente algo o hacer que el sistema no sea seguro. Además, un usuario privilegiado podría ejecutar accidentalmente un programa o código en un sitio web que podría realizar un cambio malicioso en el sistema sin su conocimiento.

Usuario Ejecutivo

Un usuario ejecutivo es un ejecutivo de negocios de alto nivel, como el presidente de la empresa, el vicepresidente o el CEO. El desafío de seguridad cuando se trata de este tipo de usuarios es que generalmente requieren acceso a más recursos de la empresa que un usuario normal o incluso la administración. Dado que los usuarios ejecutivos requieren un acceso elevado a recursos específicos, es fundamental que tome medidas para proteger sus cuentas con contramedidas como contraseñas seguras, caducidad de contraseñas y autenticación de dos factores.

Roles y responsabilidades de los datos

Varios roles diferentes interactúan con los datos de una organización. Para el examen Security+, debe estar familiarizado con los siguientes roles de datos:

■ **Propietario de los** datos El propietario de los datos suele ser el propietario de la empresa, el equipo ejecutivo o el jefe de departamento que decide qué datos se consideran un activo y cómo deben protegerse esos datos.

■ **Custodio / administrador de datos** El custodio (también conocido como administrador) es la persona que implementa el control de seguridad basado en el valor del activo determinado por el propietario. El custodio es el administrador de TI que realiza tareas comunes como copias de seguridad, configuración de permisos, configuración de firewalls y sistemas de endurecimiento.

Recuerde que el propietario determina los controles necesarios, mientras que el custodio realmente asegura el activo mediante la implementación de esos controles.

■ **Oficial de privacidad de datos (DPO)** El oficial de privacidad, también conocido como director de privacidad (CPO), es responsable de desarrollar políticas que aborden los datos personales de los empleados y los datos personales de los clientes. La política de privacidad debe especificar cómo se deben manejar y almacenar los datos personales dentro de la organización.

Para el examen, conozca los diferentes roles y responsabilidades de seguridad. Recuerde especialmente el papel del propietario de los datos, el custodio de los datos, el controlador de datos y el procesador de datos.

Oficial de Seguridad

El oficial de seguridad tiene un papel muy importante y es el enlace entre la gerencia (el propietario) y el personal de TI (custodio). El oficial de seguridad es responsable de asegurarse de que se sigan las políticas educando a todos sobre su papel dentro de la organización.

El oficial de seguridad tiene el desafío de ayudar a la gerencia a comprender el valor de los controles de seguridad implementados al asegurarse de que comprendan sus responsabilidades legales y los beneficios financieros de implementar los controles.

EJERCICIO 2-2

Terminología de seguridad

En este ejercicio, hará coincidir el término con la definición apropiada colocando la letra de la definición con el término.

Term	Definition
_____ Custodian	A. Upper-level management
_____ Confidentiality	B. A threat intelligence source that automates the collection of contact information and IoT devices on the Internet for your company
_____ Owner	C. A solution to increase availability
_____ Separation of duties	D. Persons who deploy IT systems or solutions without the knowledge and permission of the IT department
_____ Rotation of duties	E. Critical tasks divided into different jobs, with each person performing one of the different jobs
_____ RAID	F. Performs a highly comprehensive, well-planned attack that gives the attacker long-term access to the target system
_____ Integrity	G. Limiting fraudulent activities by employees by having someone else take over the job within a certain amount of time
_____ Shadow IT	H. Ensuring that data is valid
_____ APT	I. The IT staff
_____ OSINT	J. Keeping information secret

RESUMEN DE LA CERTIFICACIÓN

En este capítulo ha aprendido términos y principios de seguridad que le ayudarán a responder las preguntas relacionadas con el examen de certificación Security+, pero que también sentarán las bases para capítulos posteriores de este libro. A continuación, se resumen algunos puntos clave sobre los conceptos y principios de seguridad que ha aprendido:

■ Los objetivos fundamentales de la seguridad son la confidencialidad, la integridad y la disponibilidad (CIA).

■ Antes de que un usuario se autentique en un sistema, debe identificarse en el sistema. Un método típico para identificar a un usuario es dándole un nombre de usuario único.

■ La autorización viene después de la autenticación y, por lo general, implica dar a los usuarios acceso a los recursos apropiados. La asignación de permisos es un ejemplo de autorización de usuarios.

■ Hay muchos tipos de seguridad, como la seguridad física, la seguridad de las comunicaciones, la seguridad informática y la seguridad de la red.

■ El principio de privilegios mínimos significa que usted otorga solo el nivel mínimo de privilegios o derechos necesarios para realizar una tarea.

■ El propósito de la separación de funciones es garantizar que las tareas críticas se divida en trabajos separados y que cada trabajo sea realizado por una persona diferente. Esto ayudará a garantizar la integridad de la tarea.

■ La rotación de tareas garantiza que usted rota a los empleados a través de diferentes puestos de forma regular. Esto ayuda a prevenir y detectar actividades fraudulentas por parte del empleado que anteriormente estaba en el puesto.

Con una sólida comprensión del material presentado en este capítulo, no tendrá ningún problema con ninguna pregunta relacionada en su examen. El material presentado aquí no solo es importante para el examen, sino que también presenta términos importantes con los que debe familiarizarse para los capítulos restantes de este libro.

✓ SIMULACRO DE DOS MINUTOS

Objetivos de la seguridad de la información

❑Los objetivos de la seguridad de la información son la confidencialidad, la integridad y la disponibilidad (CIA).

❑La confidencialidad implica mantener los datos y las comunicaciones privadas a las partes involucradas. El método más popular para implementar la confidencialidad es el cifrado, pero también puede ayudar a mantener la confidencialidad mediante el uso de permisos.

❑Integridad significa garantizar que los datos se conserven en su estado original y no se modifiquen. Normalmente, la integridad de los datos se mantiene a través de un algoritmo hash, que es una operación matemática utilizada en los datos para generar una respuesta (valor hash). A continuación, este valor hash se compara con el momento en que desea verificar la integridad de los datos.

❑La disponibilidad se ocupa de garantizar que los datos estén disponibles cuando sea necesario. Ejemplos populares de tecnologías para ayudar con la disponibilidad son las copias de seguridad, RAID y la tecnología de clústeres.

❑La rendición de cuentas se ha convertido en un objetivo importante de la seguridad de la información, y se trata de poder responsabilizar a los usuarios por sus acciones. Puede implementar la responsabilidad mediante el registro y la auditoría dentro de su entorno.

Descripción de la autenticación y la autorización

❑El proceso para obtener acceso a los recursos en cualquier entorno es identificar, autenticar y, a continuación, autorizar.

❑La identificación trata de que los usuarios en la red primero se identifiquen a sí mismos, normalmente mediante el uso de un nombre de usuario, pero también podrían usar una insignia de identificación.

❑Una vez que el usuario es identificado en un sistema o red, se autentica proporcionando una contraseña con el nombre de usuario. A continuación, el nombre de usuario y la contraseña se comparan con un servidor de autenticación para comprobar que las credenciales proporcionadas son correctas.

❑Una vez autenticado el usuario, la autorización se activa. Con la autorización, se permite o no se permite al usuario acceder a los recursos basados en la lista de control de acceso (ACL) asociada con el recurso. Un ejemplo de una ACL es una lista de permisos en una carpeta.

Comprender los principios y la terminología de seguridad

❑Los diferentes tipos de seguridad incluyen seguridad física, seguridad de comunicaciones, seguridad informática y seguridad de red.

❑La seguridad física se ocupa de controlar quién puede obtener acceso físico a un sistema o instalación. La seguridad de la comunicación se ocupa de proteger los datos en tránsito, generalmente cifrando la comunicación. La seguridad informática se ocupa de implementar controles para proteger un sistema, mientras que la seguridad de red se ocupa de implementar controles para proteger la red.

❑Para el examen, asegúrese de estar familiarizado con los conceptos de privilegio mínimo, separación de deberes y rotación de deberes. El concepto de privilegio mínimo es asegurarse de que solo otorgue los privilegios mínimos necesarios para realizar una tarea. El principio de separación de funciones es garantizar que todas las tareas críticas se dividan en múltiples trabajos y que cada trabajo sea realizado por una persona diferente. La rotación de tareas es un método para mantener a los empleados honestos en sus actividades al rotar a diferentes empleados a través del rol de trabajo de forma regular.

❑El concepto de necesidad de saber es garantizar que la información esté disponible y se dé sólo a las personas que necesitan conocer esa información.

❑Un aspecto importante de la seguridad de la información es asegurarse de adoptar un enfoque en capas mediante la implementación de diferentes controles de seguridad para proteger su entorno. Por ejemplo, asegúrese de usar más que un firewall: debe usar un firewall, soluciones antivirus, autenticación, permisos y sistemas de detección de intrusiones, por nombrar algunas capas.

❑ Hay una serie de razones para las vulnerabilidades en el software, como el manejo inadecuado de la entrada, el manejo inadecuado de errores y la configuración incorrecta del software. Si no se codifica correctamente, su software también podría ser vulnerable a fugas de

memoria o desbordamientos de búfer, lo que podría resultar en acceso no autorizado al sistema.

❑Hay una serie de diferentes actores de amenazas (alguien que podría causar una amenaza) a tener en cuenta. Tenga en cuenta los diferentes tipos de hackers y también sepa que necesita proteger los activos de la empresa tanto de las amenazas internas, como un empleado descontento, como de las amenazas externas, como los niños de script, los hackers de sombrero negro o incluso los competidores comerciales mal intencionados.

Analizar los roles y responsabilidades de seguridad

❑Sepa que se utilizan diferentes términos para identificar los roles de seguridad de los empleados dentro de su organización.

❑El propietario del sistema o de los datos es en última instancia responsable de la seguridad de ese activo y, por lo general, es una administración de nivel superior. El propietario determina el valor del activo y también determina el nivel de protección que el activo necesita.

❑El custodio es el personal de TI responsable de implementar los controles de seguridad determinados por el propietario. El custodio realiza tareas como configurar permisos y firewalls y realizar copias de seguridad.

❑Un usuario es cualquier persona de la organización que accederá al activo a diario como parte de su función laboral.

❑Al oficial de seguridad se le asigna la tarea de garantizar que el nivel de seguridad determinado por el propietario esté siendo implementado realmente por el custodio. El oficial de seguridad será el enlace entre el propietario y el custodio.

AUTO Evaluación

Las siguientes preguntas le ayudarán a medir su comprensión del material presentado en este capítulo. Como se indicó, algunas preguntas pueden tener más de una respuesta correcta, así que asegúrese de leer todas las opciones de respuesta cuidadosamente.

Objetivos de la seguridad de la información

1. Según lo solicitado por su administrador, compra dos servidores para participar en un clúster de servidores, de modo que si un servidor falla, el otro servidor se hará cargo de la carga de trabajo. ¿Cuál de los siguientes objetivos de seguridad se ha cumplido?

A. Confidencialidad

B. Rendición de cuentas

C. Integridad

D. Disponibilidad

2. Ha protegido el contenido de un archivo altamente confidencial cifrando los datos. ¿Cuál de los siguientes objetivos de seguridad se ha cumplido?

A. Confidencialidad

B. Rendición de cuentas

C. Integridad

D. Disponibilidad

3. Ha administrado los permisos en un archivo para que personas no autorizadas no puedan realizar modificaciones en el archivo. ¿Qué objetivo de seguridad se ha cumplido?

A. Confidencialidad

B. Rendición de cuentas

C. Integridad

D. Disponibilidad

Descripción de la autenticación y la autorización

4. Ha configurado su red para que cada persona en la red debe proporcionar un nombre de usuario y contraseña para obtener acceso. Presentar un nombre de usuario es un ejemplo de _____.

A. autenticación

B. Identificación

C. autorización

D. confidencialidad

5. Ha configurado los permisos en la carpeta de contabilidad para que el grupo contabilidad pueda crear, modificar y eliminar contenido en la carpeta; el grupo Administradores puede leer el contenido de la carpeta; y a todos los demás usuarios se les deniega el acceso. Este es un ejemplo de cuál de los siguientes?

A. Autenticación

B. Identificación

C. Autorización

D. Confidencialidad

6. ¿Cuáles de los siguientes se consideran biométricos? (Elija dos.)

A. Nombre de usuario y contraseña

B. Tarjeta inteligente

C. Número PIN

D. Huella dactilar

E. Gammagrafía de retina

7. Antes de que una persona esté autorizada a acceder a los recursos de la red, primero está _____ con la red.

A. autenticado

B. identificado

C. integrado

D. cifrado

Comprender los principios y la terminología de seguridad

8. Se ha tomado el tiempo para crear e implementar políticas de seguridad dentro de su organización. Este es un ejemplo de cuál de los siguientes?

A. Diligencia debida

B. Separación de funciones

C. Privilegio mínimo

D. El debido cuidado

9. Todos los contadores deben poder modificar los datos contables, excepto Bob. Debido a los requisitos de trabajo de Bob, se ha asegurado de que reciba solo el permiso de lectura de los datos contables. Este es un ejemplo de cuál de los siguientes?

A. Rotación de funciones

B. Separación de funciones

C. Privilegio mínimo

D. El debido cuidado

10. ¿Cuál de las siguientes opciones representa el razonamiento para implementar la rotación de funciones en su entorno?

A. Para limitar las actividades fraudulentas dentro de la organización

B. Para mantener los datos privados para las personas apropiadas

C. Facilitar información

D. Velar por el secreto de la información

11. Dentro de la mayoría de las organizaciones, la persona que escribe el cheque no es la persona que firma el cheque. Este es un ejemplo de cuál de los siguientes?

A. Rotación de funciones

B. Separación de funciones

C. Privilegio mínimo

D. El debido cuidado

12. Después de crear e implementar la directiva de seguridad de la empresa, verifique que las políticas se sigan de forma regular mediante la realización de auditorías periódicas. Este es un ejemplo de cuál de los siguientes?

A. Diligencia debida

B. Separación de funciones

C. Privilegio mínimo

D. El debido cuidado

13. ¿Qué tipo de actor de amenazas utiliza las técnicas de un hacker para comprometer los sistemas de la empresa con la autorización de la empresa?

A. Sombrero negro

B. Sombrero gris

C. Sombrero blanco

D. El amarillo tiene

14. ¿Cuál de los siguientes tipos de vulnerabilidad se relaciona directamente con el programador del software? (Elija todo lo que corresponda).

A. Manejo inadecuado de la entrada

B. Configuración incorrecta/configuración débil

C. Manejo inadecuado de errores

D. Condiciones de la raza

E. Cuenta configurada incorrectamente

15. Los miembros del departamento de contabilidad han conectado un enrutador inalámbrico a la red sin el consentimiento del departamento de TI. ¿Cuál es el tipo de actor de amenazas involucrado aquí?

A. APT

B. TI en la sombra

C. Hacker de sombrero gris

D. Script kiddie

16. ¿Qué tipo de actor de amenazas ejecuta un ataque conciso y planificado, con un propósito, que generalmente implica que el hacker tenga acceso al sistema durante un largo período de tiempo?

A. TI en la sombra

B. Script Kiddie

C. Sindicatos delictivos

D. APT

Analizar los roles y responsabilidades de seguridad

17. ¿La entidad responsable de decidir el nivel de protección de los datos y que es responsable en última instancia de la seguridad de esos datos es cuál de las siguientes?

A. Custodio

B. Propietario

C. Usuario

D. Administrador

18. ¿La entidad responsable de implementar los controles de seguridad adecuados para proteger un activo es cuál de las siguientes?

A. Custodio

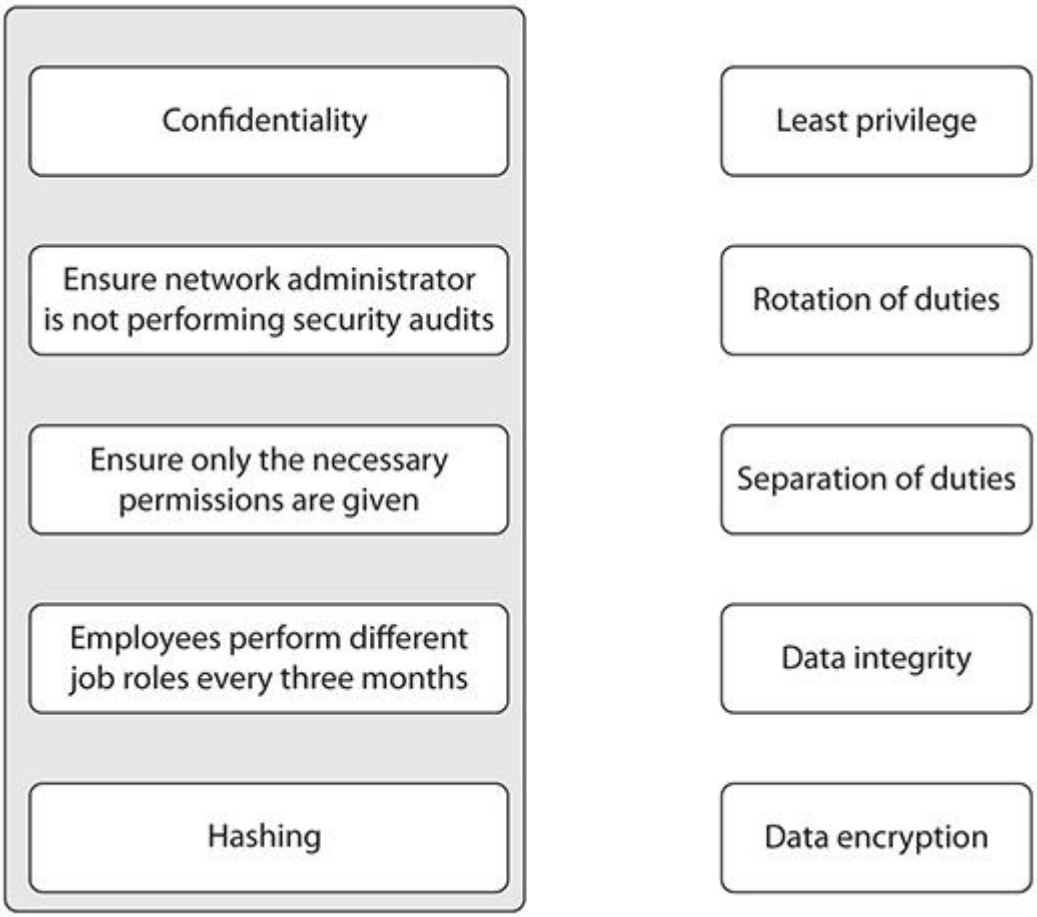
B. Propietario

C. Usuario

D. Administrador

Pregunta basada en el rendimiento

19. Usando la siguiente exhibición, haga coincidir el elemento en el lado derecho con el término o descripción correspondiente en el lado izquierdo.


Confidentiality
Ensure network administrator is not performing security audits
Ensure only the necessary permissions are given
Employees perform different job roles every three months
Hashing
Least privilege
Rotation of duties
Separation of duties
Data integrity
Data encryption