# CISSP Dominio 2 - Seguridad de los activos

**Este capítulo cubre los siguientes tópicos:**

- **Conceptos de seguridad de activos : los** conceptos discutidos incluyen política de datos, roles y responsabilidades, calidad de datos y documentación y organización de datos.
- **Identificar y clasificar información y activos : los** temas de clasificación discutidos incluyen clasificación de datos y activos, sensibilidad y criticidad, clasificaciones del sector privado, clasificaciones militares y gubernamentales, el ciclo de vida de la información, bases de datos y auditoría de datos.
- **Propiedad de la información y los activos :** analiza la determinación y documentación de la propiedad de la información y los activos.
- **Proteger la privacidad : los** componentes incluyen propietarios, procesadores de datos, remanencia de datos y limitación de recopilación.
- **Retención de activos : los** conceptos de retención discutidos incluyen medios, hardware y personal.
- **Controles de seguridad de datos : los** temas incluyen seguridad de datos, estados de datos, acceso y uso compartido de datos, almacenamiento y archivo de datos, líneas de base, alcance y personalización, selección de estándares y métodos de protección de datos.
- **Requisitos de manejo de información y activos : los** temas incluyen marcado, etiquetado, almacenamiento y destrucción.

Los activos son todas las entidades que son valiosas para una organización e incluyen activos tangibles e intangibles. Como se menciona en el Capítulo 1 , " Seguridad y administración de riesgos ", los activos tangibles incluyen computadoras, instalaciones, suministros y personal. Los activos intangibles incluyen propiedad intelectual, datos y reputación organizacional. Todos los activos de una organización deben protegerse para garantizar el éxito futuro de la organización. Si bien proteger algunos activos es tan fácil como guardarlos en una caja fuerte, otros activos requieren medidas de seguridad más avanzadas.

El dominio de seguridad de activos aborda una amplia gama de temas que incluyen información y identificación y clasificación de activos, información y propiedad de activos, protección de la privacidad, retención de activos, controles de seguridad y manejo de información y activos. Del 100% del examen, este dominio tiene un peso medio del 10%, que es el peso más bajo de los dominios.

Un profesional de la seguridad debe preocuparse por todos los aspectos de la seguridad de los activos. El factor más importante para determinar los controles utilizados para garantizar la seguridad de los activos es el valor de un activo. Si bien algunos activos de la organización pueden considerarse más importantes porque tienen mayor valor, debe asegurarse de que no se olviden los activos. Este capítulo cubre todos los aspectos de la seguridad de los activos que usted, como profesional de seguridad de TI, debe comprender.

**Conceptos de seguridad de activos**

Los conceptos de seguridad de activos que debe comprender incluyen

- Política de datos
- Funciones y responsabilidades
- Calidad de los datos
- Documentación y organización de datos

**Política de datos**

Como profesional de la seguridad, debe asegurarse de que su organización implemente una política de datos que defina objetivos a largo plazo para la gestión de datos. Lo más probable es que sea necesario que cada unidad de negocio individual dentro de la organización defina su propia política de datos, basada en la política de datos general de la organización. Dentro de la política de datos, se deben definir los roles y responsabilidades individuales para garantizar que el personal comprenda sus tareas laborales en relación con la política de datos.

Una vez que se crea la política general de datos, se deben documentar las prácticas y procedimientos de gestión de datos para garantizar que se completen las tareas diarias relacionadas con los datos. Además, deben establecerse los procedimientos adecuados de garantía y control de calidad para garantizar la calidad de los datos. Deben definirse los procedimientos de almacenamiento y copia de seguridad de los datos para garantizar que los datos se puedan restaurar.

Como parte de la política de datos, cualquier base de datos implementada dentro de una organización debe diseñarse cuidadosamente en función de los requisitos del usuario y el tipo de datos que se almacenarán. Todas las bases de datos deben cumplir con las políticas de datos que se implementen.

Antes de establecer una política de datos, debe considerar varios aspectos que pueden afectarla. Estos problemas incluyen el costo, la responsabilidad, los requisitos legales y reglamentarios, la privacidad, la sensibilidad y la propiedad.

El costo de cualquier mecanismo de gestión de datos suele ser la consideración principal de cualquier organización. A menudo, las organizaciones no implementan una política de datos porque piensan que es más fácil permitir que los datos se almacenen de la forma que desee cada unidad de negocio o usuario. Sin embargo, si una organización no adopta políticas y procedimientos formales de datos, pueden surgir problemas de seguridad de los datos debido a los diferentes métodos de almacenamiento utilizados. Por ejemplo, suponga que el departamento de investigación de una organización decide implementar una base de datos de Microsoft SQL Server para almacenar todos los datos de investigación, pero la organización no tiene una política de datos. Si la base de datos se implementa sin un conocimiento profundo de los tipos de datos que se almacenarán y las necesidades del usuario, el departamento de investigación puede terminar con una base de datos que es difícil de navegar y administrar.

La responsabilidad implica proteger a la organización de problemas legales. La responsabilidad se ve afectada directamente por los requisitos legales y reglamentarios que se aplican a la

organización. Los problemas de datos que pueden causar problemas de responsabilidad incluyen el uso indebido de datos, la inexactitud de los datos, la violación de datos y la pérdida de datos.

La privacidad de los datos se determina como parte del análisis de datos. Las clasificaciones de datos deben determinarse en función del valor de los datos para la organización. Una vez que se determinan las clasificaciones de datos, se deben implementar controles de datos para garantizar que se implementen los controles de seguridad adecuados en función de las clasificaciones de datos. También se deben considerar las leyes y regulaciones de privacidad.

Los datos confidenciales son cualquier dato que podría afectar negativamente a una organización o individuo si se divulgaran al público u obtuvieran los atacantes. Al determinar la sensibilidad, debe comprender el tipo de amenazas que pueden ocurrir, la vulnerabilidad de los datos y el tipo de datos. Por ejemplo, los números de seguro social son más confidenciales que los datos de direcciones físicas.

La propiedad de los datos es el tema final que debe considerar como parte del diseño de la política de datos. Esto es particularmente importante si varias organizaciones almacenan sus datos en la misma base de datos. Una organización puede querer una seguridad completamente diferentecontroles establecidos para proteger sus datos. Comprender la propiedad legal de los datos es importante para asegurarse de diseñar una política de datos que tenga en cuenta los diferentes requisitos de varios propietarios de datos. Si bien esto suele ser una consideración cuando hay varias organizaciones involucradas, también puede ser un problema con diferentes unidades de negocios en la misma organización. Por ejemplo, los datos del departamento de recursos humanos tienen diferentes propietarios y, por lo tanto, diferentes requisitos que los datos del departamento de investigación.

Funciones y responsabilidades

Los roles que generalmente están vinculados a la seguridad de los activos son los propietarios y custodios de los datos. Los propietarios de datos son el personal que realmente posee un conjunto de datos determinado. Estos propietarios de datos determinan el nivel de acceso que cualquier usuario tiene a sus datos. Los custodios de datos son el personal que realmente gestiona el acceso a un conjunto de datos determinado. Si bien los propietarios de los datos determinan el nivel de acceso otorgado, son los custodios de los datos quienes realmente configuran los controles apropiados para otorgar o denegar el acceso del usuario, según la aprobación del propietario de los datos.

**Nota**

Ambos roles se presentan en la sección “ Roles y responsabilidades de seguridad ” del Capítulo 1 .

Propietario de los datos

Los propietarios de los datos deben comprender la forma en que se utilizan los datos de los que son responsables y cuándo deben divulgarse. También deben determinar el valor y el impacto de

los datos en la organización. El propietario de los datos debe comprender lo que se necesita para restaurar o reemplazar los datos y el costo en el que se incurrirá durante este proceso. Por último, los propietarios de los datos deben comprender cuándo los datos son inexactos o la organización ya no los necesita.

En la mayoría de los casos, cada unidad de negocio dentro de una organización designa a un propietario de datos, a quien se le debe otorgar el nivel apropiado de autoridad para los datos de los que es responsable. Los propietarios de los datos deben comprender cualquier problema de derechos de propiedad intelectual y derechos de autor de los datos. Los propietarios de los datos son responsables de garantizar que existan los acuerdos adecuados si se concede acceso a los datos a terceros.

Custodio de datos

Los custodios de datos deben comprender los niveles de acceso a los datos que se les puede dar a los usuarios. Los custodios de datos trabajan con los propietarios de los datos para determinar el nivel de acceso que se debe otorgar. Este es un excelente ejemplo de separaciones. Al tener roles separados, como propietarios y custodios de datos, una organización puede garantizar que ningún rol sea responsable del acceso a los datos. Esto evita la creación fraudulenta de cuentas de usuario y la asignación de derechos.

Los custodios de datos deben comprender las políticas y pautas de datos. Deben documentar las estructuras de datos en la organización y los niveles de acceso otorgados. También son responsables del almacenamiento, el archivo y las copias de seguridad de los datos. Por último, deben preocuparse por la calidad de los datos y, por lo tanto, deben implementar los controles de auditoría adecuados.

Los custodios de datos centralizados son comunes. Los propietarios de los datos otorgan a los custodios de los datos el nivel de permiso que se les debe otorgar a los usuarios y grupos. Los custodios de datos realmente implementan las listas de control de acceso (ACL) para los dispositivos, bases de datos, carpetas y archivos.

Calidad de los datos

*La calidad de los datos* se define como la aptitud de los datos para su uso. La calidad de los datos debe mantenerse durante todo el ciclo de vida de los datos, incluso durante la captura de datos, la modificación de datos, el almacenamiento de datos, la distribución de datos, el uso de datos y el archivo de datos. Los profesionales de la seguridad deben asegurarse de que su organización adopte las medidas de control y garantía de calidad adecuadas para que la calidad de los datos no se vea afectada. La calidad de los datos se asegura con mayor frecuencia al garantizar la integridad de los datos, que protege los datos de cambios accidentales, no autorizados o no intencionales. Con la integridad de los datos, se sabe que los datos son buenos y se puede confiar en que la información es completa, coherente y precisa. La integridad del sistema asegura que un sistema funcionará según lo previsto.

Los profesionales de seguridad deben trabajar para documentar los estándares, procesos y procedimientos de datos para monitorear y controlar la calidad de los datos. Además, los procesos internos deben diseñarse para evaluar periódicamente la calidad de los datos. Cuando los datos se almacenan en bases de datos, el control y la garantía de calidad son más fáciles de garantizar utilizando los controles de datos internos en la base de datos. Por ejemplo, puede configurar un campo numérico para permitir solo la entrada de cantidades de moneda específicas. Al hacer esto, se asegurará de que solo los valores que usen dos decimales puedan ingresarse en los campos de datos. Este es un ejemplo de validación de entrada.

La contaminación de datos ocurre cuando se introducen errores de datos. Los errores de datos se pueden reducir mediante la implementación de los mecanismos de garantía y control de calidad adecuados. La verificación de datos, una parte importante del proceso, evalúa qué tan completos y correctos son los datos y si cumplen con los estándares. La verificación de datos puede ser realizada por personal que tiene la responsabilidad de ingresar los datos. La validación de datos evalúa los datos después de que se ha realizado la verificación de datos y prueba los datos para garantizar que se cumplan los estándares de calidad de los datos. La validación de datos debe ser realizada por personal que esté más familiarizado con los datos.

Las organizaciones deben desarrollar procedimientos y procesos que mantengan dos problemas de datos clave a la vanguardia: prevención y corrección de errores. La prevención de errores se proporciona en la entrada de datos, mientras que la corrección de errores generalmente ocurre durante la verificación y validación de datos.

Organización y documentación de datos

La documentación de datos garantiza que los datos se comprendan en su nivel más básico y se puedan organizar correctamente en conjuntos de datos. Los conjuntos de datos garantizan que los datos se organizan y almacenan de manera relacional para que los datos se puedan utilizar para múltiples propósitos. Los conjuntos de datos deben recibir nombres descriptivos únicos que indiquen su contenido.

Al documentar los datos y organizar los conjuntos de datos, las organizaciones también pueden garantizar que los datos duplicados no se retengan en varias ubicaciones. Por ejemplo, el departamento de ventas puede capturar toda la información demográfica de todos los clientes. Sin embargo, el departamento de envíos también puede necesitar acceso a esta misma información demográfica para garantizar que los productos se envíen a la dirección correcta. Además, el departamento de cuentas por cobrar necesitará acceso a la información demográfica del cliente para fines de facturación. No es necesario que cada unidad de negocio tenga conjuntos de datos separados para esta información. Identificar el conjunto de datos demográficos del cliente como necesario para varias unidades de negocio evita la duplicación de esfuerzos en todas las unidades de negocio.

Dentro de cada conjunto de datos, se debe crear documentación para cada tipo de datos. En el ejemplo del conjunto de datos demográficos del cliente, se recopilan el nombre, la dirección y el número de teléfono del cliente. Para cada uno de los tipos de datos, se deben crear los parámetros individuales para cada tipo de datos. Si bien una dirección puede permitir una combinación de

números y caracteres, un número de teléfono debe permitir solo números. Además, cada tipo de datos puede tener una longitud máxima. Por último, es importante documentar qué datos se requieren, lo que significa que deben recopilarse e ingresarse. Por ejemplo, una organización puede decidir que los números de fax no son obligatorios, pero sí los números de teléfono. Recuerde que cada una de estas decisiones la toma mejor el personal que trabaja más de cerca con los datos.

Una vez que se ha producido toda la documentación, se debe mapear la organización de los datos. Esta organización incluirá todas las interrelaciones entre los conjuntos de datos. También debe incluir información sobre qué unidades de negocio necesitarán acceso a conjuntos de datos o subconjuntos de un conjunto de datos.

**Nota**

*Big data* es un término para conjuntos grandes o complejos, tan grandes o complejos que no pueden ser analizados por aplicaciones tradicionales de procesamiento de datos. Se han diseñado aplicaciones especializadas para ayudar a las organizaciones con sus macrodatos. Los desafíos de big data que se pueden encontrar incluyen análisis de datos, captura de datos, búsqueda de datos, intercambio de datos, almacenamiento de datos y privacidad de datos.

Identificar y clasificar información y activos

Los profesionales de la seguridad deben asegurarse de que las organizaciones para las que trabajan identifiquen y clasifiquen correctamente toda la información y los activos de la organización. El primer paso en este proceso es identificar toda la información y los activos que la organización posee y utiliza. Para realizar la identificación de información y activos, los profesionales de seguridad deben trabajar con los representantes de cada departamento o área funcional. Una vez que se identifican la información y los activos, los profesionales de seguridad deben realizar la clasificación de datos y activos y documentar la sensibilidad y criticidad de los datos.

Los profesionales de la seguridad deben comprender las clasificaciones del sector privado, las clasificaciones militares y gubernamentales, el ciclo de vida de la información, las bases de datos y la auditoría de datos.

Clasificación de activos y datos

Los datos y activos deben clasificarse en función de su valor para la organización y su sensibilidad a la divulgación. Asignar un valor a los datos y activos permite a una organización determinar los recursos que deben usarse para protegerlos. Los recursos que se utilizan para proteger los datos incluyen recursos de personal, recursos monetarios, recursos de control de acceso, etc. La clasificación de datos y activos le permite aplicar diferentes medidas de protección. La clasificación de datos es fundamental para todos los sistemas para proteger la confidencialidad, integridad y disponibilidad (CIA) de los datos.

Una vez que se clasifican los datos, los datos se pueden segmentar en función del nivel de protección necesario. Los niveles de clasificación aseguran que los datos se manejen y protejan de la manera más rentable posible. Luego, los activos podrían configurarse para garantizar que los datos estén aislados o protegidos en función de estos niveles de clasificación. Una organización debe determinar los niveles de clasificación que utiliza en función de las necesidades de la organización. Se utilizan comúnmente varias clasificaciones del sector privado y clasificaciones de información militar y gubernamental.

**Nota**

Las clasificaciones comunes del sector privado y las clasificaciones militares y gubernamentales se analizan más adelante en esta sección.

El ciclo de vida de la información, que se trata con más detalle más adelante en este capítulo, también debe basarse en la clasificación de los datos. Se requiere que las organizaciones retengan cierta información, particularmente datos financieros, según las leyes y regulaciones locales, estatales o gubernamentales.

Sensibilidad y criticidad

*La sensibilidad* es una medida de la libertad con la que se pueden manejar los datos. Algunos datos requieren un cuidado y manejo especiales, especialmente cuando un manejo inadecuado podría resultar en sanciones,robo de identidad, pérdida financiera, invasión de la privacidad o acceso no autorizado por parte de una persona o muchas personas. Algunos datos también están sujetos a la regulación de las leyes estatales o federales y requieren notificación en caso de divulgación.

A los datos se les asigna un nivel de sensibilidad en función de quién debería tener acceso a ellos y cuánto daño se produciría si se divulgaran. Esta asignación de sensibilidad se denomina *clasificación de datos* .

*La criticidad* es una medida de la importancia de los datos. Los datos que se consideran confidenciales no necesariamente se consideran críticos. Asignar un nivel de criticidad a un conjunto de datos en particular requiere considerar las respuestas a algunas preguntas:

- ¿Podrá recuperar los datos en caso de desastre?
- ¿Cuánto tiempo llevará recuperar los datos?
- ¿Cuál es el efecto de este tiempo de inactividad, incluida la pérdida de prestigio público?

Los datos se consideran esenciales cuando son críticos para el negocio de la organización. Cuando los datos esenciales no están disponibles, incluso por un breve período de tiempo, o cuando su integridad es cuestionable, la organización no puede funcionar. Los datos se consideran necesarios cuando son importantes para la organización, pero las operaciones de la organización continuarían durante un período de tiempo predeterminado, incluso si los datos no estuvieran disponibles. Los datos no son esenciales si la organización puede operar sin ellos durante períodos prolongados.

Una vez que se comprenden y documentan la sensibilidad y la criticidad de los datos, la organización debe trabajar para crear un sistema de clasificación de datos. La mayoría de las organizaciones utilizarán un sistema de clasificación del sector privado o un sistema de clasificación militar y gubernamental.

PII

La información de identificación personal (PII) se definió y explicó en el Capítulo 1 . La PII se considera información que debe clasificarse y protegerse. La Publicación Especial (SP) 800-122 del Instituto Nacional de Estándares y Tecnología (NIST) brinda pautas sobre la protección de la confidencialidad de la PII.


Según SP 800-122, las organizaciones deben implementar las siguientes recomendaciones para proteger eficazmente la PII:

- Las organizaciones deben identificar toda la PII que reside en su entorno.
- Las organizaciones deben minimizar el uso, recopilación y retención de PII a lo estrictamente necesario para lograr su propósito y misión comercial.
- Las organizaciones deben clasificar su PII según el nivel de impacto de confidencialidad de PII.
- Las organizaciones deben aplicar las salvaguardas adecuadas para la PII según el nivel de impacto de la confidencialidad de la PII.
- Las organizaciones deben desarrollar un plan de respuesta a incidentes para manejar las infracciones que involucren PII.
- Las organizaciones deben fomentar una estrecha coordinación entre sus directores de privacidad, los principales funcionarios de la agencia para la privacidad, los directores de información, los directores de seguridad de la información y los asesores legales al abordar cuestiones relacionadas con la PII.

SP 800-122 define PII como “cualquier información sobre una persona mantenida por una agencia, incluida (1) cualquier información que pueda usarse para distinguir o rastrear la identidad de una persona, como nombre, número de seguro social, fecha y lugar de nacimiento, apellido de soltera de la madre o registros biométricos; y (2) cualquier otra información que esté vinculada o pueda vincularse a un individuo, como información médica, educativa, financiera y laboral ". Distinguir a un individuo es identificar a un individuo. Rastrear a un individuo es procesar información suficiente para tomar una determinación sobre un aspecto específico de las actividades o el estado de un individuo. La información vinculada es información sobre o relacionada con un individuo que está lógicamente asociada con otra información sobre el individuo. A diferencia de,

A toda la PII se le debe asignar niveles de impacto de confidencialidad basados en las designaciones FIPS 199. Esas designaciones son

- BAJO si se puede esperar que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.
- MODERADA si se puede esperar que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.
- ALTA si se puede esperar que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización o las personas.

La determinación del impacto de una pérdida de confidencialidad de la PII debe tener en cuenta factores relevantes. Varios factores importantes que las organizaciones deben considerar son los siguientes:

- **Identificabilidad: la** facilidad con la que se puede utilizar la PII para identificar a individuos específicos
- **Cantidad de PII:** cuántas personas se identifican en la información
- **Sensibilidad del campo de datos:** la sensibilidad de cada campo de datos de PII individual, así como la sensibilidad de los campos de datos de PII juntos
- **Contexto de uso:** el propósito para el cual se recopila, almacena, utiliza, procesa, divulga o difunde la PII.
- **Obligación de proteger la confidencialidad: las** leyes, regulaciones, estándares y prácticas operativas que dictan la responsabilidad de una organización para proteger la PII
- **Acceso y ubicación de la PII:** la naturaleza del acceso autorizado a la PII

La PII debe protegerse mediante una combinación de medidas, que incluyen salvaguardas operativas, salvaguardas específicas de privacidad y controles de seguridad. Las salvaguardas operativas deben incluir la creación de políticas y procedimientos y programas de concientización, capacitación y educación. Las salvaguardas específicas de privacidad ayudan a las organizaciones a recopilar, mantener, usar y difundir datos de manera que protejan la confidencialidad de los datos e incluyen minimizar el uso, recopilación y retención de PII; realizar evaluaciones de impacto en la privacidad; información de desidentificación; y anonimizar la información. Los controles de seguridad incluyen separación de funciones, privilegio mínimo, auditoría, identificación y autorización, y otros de NIST SP 800-53.

**Nota**

NIST SP 800-53 se trata con más detalle en el Capítulo 1 .

Las organizaciones que recopilan, usan y conservan la PII deben usar NIST SP 800-122 para ayudar a guiar los esfuerzos de la organización para proteger la confidencialidad de la PII.

FI

La información médica protegida (PHI), también conocida como información médica protegida electrónica (EPHI o ePHI), es cualquier información médica identificable individualmente. NIST SP 800-66 proporciona pautas para implementar la regla de seguridad de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). La regla de seguridad se aplica a las siguientes entidades cubiertas:

- **Proveedores de atención médica cubiertos:** cualquier proveedor de suministros o servicios médicos u otros servicios de salud que transmite información médica en forma electrónica en relación con una transacción para la cual el HHS (Departamento de Salud y Servicios Humanos de EE. UU.) Ha adoptado un estándar.
- **Planes de salud:** cualquier plan individual o grupal que proporciona o paga el costo de la atención médica (por ejemplo, un emisor de seguro de salud y los programas de Medicare y Medicaid).
- **Cámaras de compensación de atención médica:** una entidad pública o privada que procesa las transacciones de atención médica de otra entidad desde un formato estándar a un formato no estándar, o viceversa.
- **Patrocinadores de tarjetas de medicamentos recetados de Medicare:** una entidad no gubernamental que ofrece un programa de medicamentos con descuento respaldado por la Ley de Modernización de Medicare.

Cada entidad cubierta debe garantizar la confidencialidad, integridad y disponibilidad de la PHI que crea, recibe, mantiene o transmite; proteger contra cualquier amenaza y peligro razonablemente anticipado a la seguridad o integridad de EPHI; y proteger contra usos o divulgaciones razonablemente anticipados de dicha información que no están permitidos por la Regla de Privacidad.

La regla de seguridad se divide en seis secciones principales de la siguiente manera:

- **Normas de seguridad Normas generales:** incluye los requisitos generales que deben cumplir todas las entidades cubiertas; establece flexibilidad de enfoque; identifica estándares y especificaciones de implementación (tanto requeridas como direccionables); describe las decisiones que debe tomar una entidad cubierta con respecto a las especificaciones de implementación direccionables; y requiere el mantenimiento de medidas de seguridad para continuar con la protección razonable y apropiada de la PHI.
- **Salvaguardias Administrativas:** Definidas en la Regla de Seguridad como las “acciones y políticas administrativas y procedimientos para gestionar la selección, desarrollo, implementación y mantenimiento de medidas de seguridad para proteger la información médica protegida electrónica y para gestionar la conducta de la fuerza laboral de la entidad cubierta en relación a la protección de esa información ".
- **Salvaguardias físicas:** definidas como las "medidas, políticas y procedimientos físicos para proteger los sistemas de información electrónica de una entidad cubierta y los edificios y equipos relacionados de los peligros naturales y ambientales y la intrusión no autorizada".
- **Salvaguardias técnicas:** Definidas como "la tecnología y la política y los procedimientos para su uso que protegen la información médica protegida electrónica y controlan el acceso a la misma".

- **Requisitos organizativos:** incluye normas para contratos de socios comerciales y otros acuerdos, incluidos memorandos de entendimiento entre una entidad cubierta y un socio comercial cuando ambas entidades son organizaciones gubernamentales; y requisitos para planes de salud grupales.
- **Políticas y procedimientos y requisitos de documentación:** Requiere la implementación de políticas y procedimientos razonables y apropiados para cumplir con los estándares, especificaciones de implementación y otros requisitos.de la Regla de Seguridad; mantenimiento de documentación y / o registros escritos (que pueden ser electrónicos) que incluyen políticas, procedimientos, acciones, actividades o evaluaciones requeridas por la Regla de seguridad; y requisitos de conservación, disponibilidad y actualización relacionados con la documentación.

NIST SP 800-66 incluye un enlace del Marco de gestión de riesgos (RMF) de NIST y la regla de seguridad. También incluye actividades clave que deben llevarse a cabo para cada una de las seis secciones principales enumeradas anteriormente de la Regla de seguridad. Las organizaciones que recopilan, usan y conservan la PHI deben usar NIST SP 800-66 para ayudar a guiar los esfuerzos de la organización para brindar confidencialidad, integridad y disponibilidad para la PHI.

Datos de propiedad

Los datos patentados se definen como datos o documentos generados internamente que contienen información técnica o de otro tipo controlada por una organización para salvaguardar su ventaja competitiva. Los datos de propiedad pueden estar protegidos por leyes de derechos de autor, patentes o secretos comerciales. Si bien no existen estándares que rijan la protección de los datos patentados, las organizaciones deben garantizar que la confidencialidad, integridad y disponibilidad de los datos patentados estén protegidas. Debido a esto, muchas organizaciones protegen los datos de propiedad con los mismos tipos de controles que se utilizan para la PII y la PHI.

Los profesionales de la seguridad deben asegurarse de que los datos patentados se identifiquen y categoricen adecuadamente para garantizar que se implementen los controles adecuados.

Clasificaciones del sector privado


Las organizaciones del sector privado pueden clasificar los datos utilizando cuatro niveles de clasificación principales, enumerados desde el nivel de sensibilidad más alto al más bajo:

1. Confidencial
2. Privado
3. Sensitivo
4. Público

**Nota**

Depende de cada organización determinar el número y tipo de clasificaciones. Otras opciones incluyen "protegido" para indicar datos protegidos legalmente y "propietario" para indicar datos propiedad de la empresa (en un sentido legal).

Los datos que son confidenciales incluyen secretos comerciales, datos intelectuales, código de programación de aplicaciones y otros datos que podrían afectar seriamente a la organización si ocurriera una divulgación no autorizada. Los datos a este nivel solo estarían disponibles para el personal de la organización cuyo trabajo se relacione con el sujeto de los datos. Acceso a confidenciallos datos generalmente requieren autorización para cada acceso. En la mayoría de los casos, la única forma en que las entidades externas tienen acceso autorizado a datos confidenciales es la siguiente:

- Después de firmar un acuerdo de confidencialidad
- Al cumplir con una orden judicial
- Como parte de un proyecto gubernamental o un acuerdo de contratación pública

Los datos que son privados incluyen cualquier información relacionada con el personal, incluidos los registros de recursos humanos, los registros médicos y la información salarial, que solo se utiliza dentro de la organización. Los datos confidenciales incluyen información financiera de la organización y requieren medidas adicionales para garantizar su CIA y su precisión. Los datos públicos son datos que no causarían un impacto negativo en la organización.

Clasificaciones militares y gubernamentales


Las entidades militares y gubernamentales suelen clasificar los datos utilizando cinco niveles de clasificación principales, enumerados desde el nivel de sensibilidad más alto al más bajo:

1. **Alto secreto: la** divulgación causaría un peligro excepcionalmente grave para la seguridad nacional.
2. **Secreto: la** divulgación causaría graves daños a la seguridad nacional.
3. **Confidencial: la** divulgación causaría daños a la seguridad nacional.
4. **Sensible pero no clasificado: la** divulgación podría dañar la seguridad nacional.
5. **Sin clasificar:** cualquier información que, en general, pueda distribuirse al público sin ninguna amenaza para el interés nacional.

Las agencias federales de EE. UU. Utilizan la designación Sensible pero no clasificada (SBU) cuando la información no está clasificada pero aún necesita protección y requiere controles estrictos sobre su distribución. Hay más de 100 etiquetas diferentes para SBU, que incluyen:

- Sólo para uso oficial

- Uso oficial limitado
- Información de seguridad sensible
- Información de infraestructura crítica

La orden ejecutiva 13556 creó una designación estándar Información no clasificada controlada (CUI). La implementación está en progreso.

Los datos de alto secreto incluyen planos de armas, especificaciones de tecnología, información de satélites espías y otra información militar que podría dañar gravemente seguridad nacional si se divulga. Los datos que son secretos incluyen planes de despliegue, ubicación de misiles y otra información que podría dañar seriamente la seguridad nacional si se divulga. Los datos que son confidenciales incluyen la fuerza de las fuerzas en los Estados Unidos y en el extranjero, información técnica utilizada para capacitación y mantenimiento, y otra información que podría afectar seriamente al gobierno si ocurriera una divulgación no autorizada. Los datos que son sensibles pero no clasificados incluyen datos médicos u otros datos personales que podrían no causar un daño grave a la seguridad nacional si se divulgan, pero que podrían hacer que los ciudadanos cuestionen la reputación del gobierno. La información militar y gubernamental que no se incluye en ninguna de las otras cuatro categorías se considera no clasificada y, por lo general, debe entregarse al público de acuerdo con la Ley de Libertad de Información.

**Nota**

Promulgada el 4 de julio de 1966 y que entrará en vigor un año después, la Ley de Libertad de Información (FOIA) proporciona una herramienta poderosa para los defensores del acceso a la información. Según la FOIA, cualquier persona puede solicitar y recibir registros de agencias federales a menos que los documentos se declaren oficialmente exentos en función de categorías específicas, como alto secreto, secreto y confidencial. Para obtener más información sobre cómo explorar los datos de la FOIA o realizar una solicitud de la FOIA, visite https://www.foia.gov .

Ciclo de vida de la información

Las organizaciones deben asegurarse de que toda la información que recopilen y almacenen se gestione durante todo el ciclo de vida de esa información. Si no se sigue el ciclo de vida de la información, el almacenamiento requerido para la información aumentará con el tiempo hasta que se necesiten más recursos de almacenamiento. Por lo tanto, los profesionales de la seguridad deben asegurarse de que los propietarios y custodios de los datos comprendan el ciclo de vida de la información.


Para la mayoría de las organizaciones, las cinco fases del ciclo de vida de la información son las siguientes:

1. Crear / recibir

2. Distribuir
3. Usar
4. Mantener
5. Desechar / almacenar

Durante la fase de creación / recepción, los datos son creados por el personal de la organización o recibidos por la organización a través del portal de entrada de datos. Si los datos los crea el personal de la organización, generalmente se colocan en la ubicación desde la cual se distribuirán, usarán y mantendrán. Sin embargo, si los datos se reciben a través de algún otro mecanismo, puede ser necesario copiar o importar los datos a unlocalización. En este caso, los datos no estarán disponibles para distribución, uso y mantenimiento hasta después de la copia o importación.

Después de la fase de creación / recepción, el personal de la organización debe asegurarse de que los datos se distribuyan correctamente. En la mayoría de los casos, esto implica colocar los datos en la ubicación adecuada y posiblemente configurar los permisos de acceso según lo definido por el propietario de los datos. No obstante, tenga en cuenta que, en muchos casos, es posible que ya se hayan configurado la ubicación de almacenamiento y los permisos adecuados de usuario y grupo. En tal caso, solo es cuestión de asegurarse de que los datos estén en la ubicación de distribución correcta. Las ubicaciones de distribución incluyen bases de datos, carpetas compartidas, almacenamiento conectado a la red (NAS), redes de área de almacenamiento (SAN) y bibliotecas de datos.

Una vez que se han distribuido los datos, el personal de la organización puede utilizar los datos en sus operaciones diarias. Si bien algunos miembros del personal solo tendrán acceso de lectura a los datos, otros pueden tener permisos de escritura o de control total. Recuerde que los permisos permitidos o denegados son designados por el propietario de los datos, pero configurados por el custodio de los datos.

Ahora que los datos se utilizan en las operaciones diarias, el mantenimiento de los datos es clave para garantizar que los datos permanezcan accesibles y seguros. El mantenimiento incluye la auditoría, la realización de copias de seguridad, la supervisión del rendimiento y la gestión de datos.

Una vez que los datos han llegado al final del ciclo de vida, debe desecharlos correctamente o asegurarse de que estén almacenados de forma segura. Algunas organizaciones deben mantener registros de datos durante un cierto número de años según las leyes o regulaciones locales, estatales o federales. Este tipo de datos debe archivarse durante el período requerido. Además, todos los datos que forman parte de un litigio deben conservarse según lo solicite el tribunal de justicia, y las organizaciones deben seguir los procesos de documentación de pruebas y la cadena de custodia adecuada. La organización debe definir claramente los procedimientos de archivo y destrucción de datos.

Todas las organizaciones necesitan procedimientos para la retención y destrucción de datos. La retención y destrucción de datos deben seguir todas las leyes y regulaciones locales, estatales y gubernamentales. La documentación de los procedimientos adecuados garantiza que la

información se mantenga durante el tiempo necesario para evitar multas económicas y el posible encarcelamiento de los funcionarios de la organización de alto nivel. Estos procedimientos deben incluir tanto el período de retención como el proceso de destrucción.

La figura 2-1 muestra el ciclo de vida de la información.

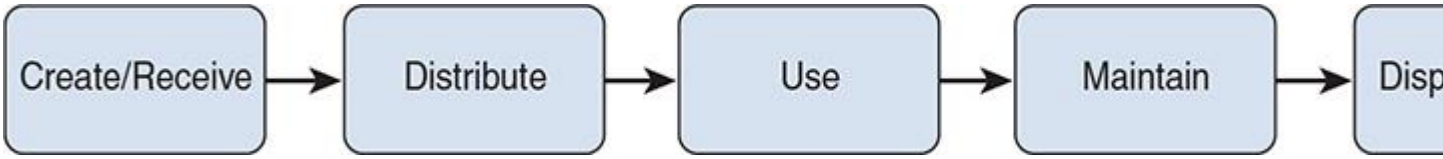


**Figura 2-1** Ciclo de vida de la información

Bases de datos

Las bases de datos se han convertido en la tecnología preferida para almacenar, organizar y analizar grandes conjuntos de datos. Los usuarios generalmente acceden a una base de datos a través de una interfaz de cliente. A medida que surge la necesidad de proporcionar acceso a entidades externas a la empresa, aumentan las oportunidades de uso indebido. En esta sección, se tratan los conceptos necesarios para discutir la seguridad de la base de datos, así como las preocupaciones de seguridad relacionadas con la administración y el mantenimiento de la base de datos.

Arquitectura y modelos de DBMS

Las bases de datos contienen datos y la principal diferencia en los modelos de bases de datos es cómo se almacena y organiza esa información. El modelo describe las relaciones entre los elementos de datos, cómo se accede a los datos, cómo se asegura la integridad y operaciones aceptables. Los cinco modelos o arquitecturas que discutimos son

- Relacional
- Jerárquico
- La red
- Orientado a objetos
- Objeto-relacional

El modelo *relacional* utiliza *atributos* (columnas) y *tuplas* (filas) para organizar los datos en tablas bidimensionales. Cada celda de la tabla, que representa la intersección de un atributo y una tupla, representa un registro.

Cuando trabaje con sistemas de administración de bases de datos relacionales (RDBMS), debe comprender los siguientes términos:

- **Relación :** entidad fundamental en una base de datos relacional en forma de tabla.
- **Tupla:** una fila en una tabla.
- **Atributo:** una columna en una tabla.
- **Esquema :** descripción de una base de datos relacional.

- **Registro :** una colección de elementos de datos relacionados.
- **Relación base :** en SQL, una relación que existe realmente en la base de datos.
- **Ver :** el conjunto de datos disponibles para un usuario determinado. La seguridad se refuerza mediante el uso de vistas.
- **Grado :** el número de columnas en una tabla.
- **Cardinalidad :** el número de filas en una relación.
- **Dominio :** el conjunto de valores permitidos que puede tomar un atributo.
- **Clave principal:** columnas que hacen que cada fila sea única.
- **Clave externa :** un atributo en una relación que tiene valores que coinciden con la clave principal en otra relación. Las coincidencias entre la clave externa y la clave principal son importantes porque representan referencias de una relación a otra y establecen la conexión entre estas relaciones.
- **Clave candidata :** un atributo en una relación que tiene valores que coinciden con la clave principal en otra relación.
- **Integridad referencial :** Requiere que para cualquier atributo de clave externa, la relación referenciada debe tener una tupla con el mismo valor para su clave primaria.

Un elemento importante del diseño de una base de datos que asegura que los atributos de una tabla dependan solo de la clave principal es un proceso llamado *normalización* . La normalización incluye

- Eliminar grupos repetidos colocándolos en tablas separadas
- Eliminando datos redundantes (que ocurren en más de una tabla)
- Eliminar atributos en una tabla que no dependen de la clave principal de esa tabla

En el modelo *jerárquico* , los datos se organizan en una jerarquía. Un objeto puede tener un hijo (un objeto que es un subconjunto del objeto principal), varios hijos o ningún hijo. Para navegar por esta jerarquía, debe conocer la rama en la que se encuentra el objeto. Un ejemplo del uso de este sistema es el registro de Windows y un directorio de Protocolo ligero de acceso a directorios (LDAP).

En el modelo de *red* , como en el modelo jerárquico, los datos se organizan en una jerarquía pero, a diferencia del modelo jerárquico, los objetos pueden tener múltiples padres. Debido a esto, no es necesario saber en qué rama encontrar un elemento de datos porque normalmente habrá múltiples rutas hacia él.

El modelo *orientado a objetos* tiene la capacidad de manejar una variedad de tipos de datos y es más dinámico que una base de datos relacional. Los sistemas de bases de datos orientadas a objetos (OODB) son útiles para almacenar y manipular datos complejos, como imágenes y gráficos. En consecuencia, las aplicaciones complejas que involucran multimedia, diseño asistido por computadora (CAD), video, gráficos y sistemas expertos son más adecuadas para el modelo orientado a objetos. También tiene las características de facilidad de reutilización de código y análisis y mantenimiento reducido.

Los objetos se pueden crear según sea necesario, y los datos y los procedimientos (o métodos) van con el objeto cuando se solicita. Un *método* es el código que define las acciones queel objeto

actúa en respuesta a un mensaje. Este modelo utiliza algunos de los mismos conceptos de un modelo relacional. En el modelo orientado a objetos, una relación, columna y tupla (términos relacionales) se denominan objetos de clase, atributo e instancia.

El modelo *relacional de objetos* es el matrimonio de tecnologías relacionales y orientadas a objetos, combinando los atributos de ambos. Se trata de una base de datos relacional con una interfaz de software que está escrita en un lenguaje de programación orientada a objetos (OOP). La lógica y los procedimientos se derivan del software front-end en lugar de la base de datos. Esto significa que cada aplicación de front-end puede tener sus propios procedimientos específicos.

Idiomas de la interfaz de la base de datos

El acceso a la información en una base de datos se facilita mediante una aplicación que le permite obtener e interactuar con los datos. Estas interfaces se pueden escribir en varios idiomas diferentes. Esta sección analiza algunos de los lenguajes de programación de datos más importantes:

- **ODBC :** Open Database Connectivity (ODBC) es una interfaz de programación de aplicaciones (API) que permite la comunicación con bases de datos de forma local o remota. Una API en el cliente envía solicitudes a la API de ODBC. La API de ODBC ubica la base de datos y un controlador específico convierte la solicitud en un comando de base de datos que la base de datos específica comprenderá.
- **JDBC :** como cabría esperar del título, Java Database Connectivity (JDBC) hace posible que las aplicaciones Java se comuniquen con una base de datos. Una API de Java es lo que permite a los programas Java ejecutar sentencias SQL. Es independiente de la base de datos y permite la comunicación con varios tipos de bases de datos. Proporciona la misma funcionalidad que ODBC.
- **XML : los** datos ahora se pueden crear en formato XML: Extensible Markup Language, pero la API XML: DB permite que las aplicaciones XML interactúen con bases de datos más tradicionales, como bases de datos relacionales. Requiere que la base de datos tenga un controlador específico de la base de datos que encapsule toda la lógica de acceso a la base de datos.
- **OLE DB :** Object Linking and Embedding Database (OLE DB) es un reemplazo de ODBC, extendiendo su funcionalidad a bases de datos no relacionales. Aunque está basado en COM y limitado a herramientas basadas en Microsoft Windows, proporciona a las aplicaciones un acceso uniforme a una variedad de fuentes de datos, incluido el servicio a través de objetos ActiveX.

Almacenes de datos y minería de datos

El almacenamiento de datos es el proceso de combinar datos de varias bases de datos o fuentes de datos en una ubicación central llamada almacén. El almacén se utiliza para realizar análisis. Los datos no se combinan simplemente, sino que se procesan y presentan de una manera másforma útil y comprensible. Los almacenes de datos requieren una seguridad estricta porque los datos no están dispersos sino ubicados en una ubicación central.

La minería de datos es el proceso de utilizar herramientas especiales para organizar los datos en un formato que facilita la toma de decisiones comerciales basadas en el contenido. Analiza grandes conjuntos de datos en un almacén de datos para encontrar patrones no obvios. Estas herramientas localizan asociaciones entre datos y correlacionan estas asociaciones en metadatos. Permite realizar inferencias más sofisticadas (a veces llamadas inteligencia empresarial [BI]) sobre los datos. Se deben tomar tres medidas al utilizar aplicaciones de almacenamiento de datos:

- Evite que los metadatos se utilicen de forma interactiva.
- Supervise el plan de depuración de datos.
- Concilie los datos transferidos entre el entorno de operaciones y el almacén de datos.

Mantenimiento de base de datos

Los administradores de la base de datos deben realizar el mantenimiento de la base de datos con regularidad. Las bases de datos deben respaldarse con regularidad. Todos los parches de seguridad y actualizaciones para el hardware y el software, incluido el software de la base de datos, deben mantenerse actualizados. Las actualizaciones de hardware y software son necesarias a medida que aumentan las necesidades organizativas y avanza la tecnología.

Los profesionales de la seguridad deben trabajar con los administradores de bases de datos para garantizar que el análisis de amenazas para las bases de datos se realice al menos una vez al año. También deben trabajar para desarrollar las mitigaciones y controles apropiados para protegerse contra las amenazas identificadas.

Amenazas de bases de datos

Las amenazas a la seguridad de las bases de datos generalmente giran en torno al acceso no deseado a los datos. Dos amenazas a la seguridad que existen en la gestión de bases de datos involucran los procesos de *agregación* e *inferencia* . La agregación es el acto de combinar información de varias fuentes. La forma en que esto puede convertirse en un problema de seguridad con las bases de datos es cuando un usuario no tiene acceso a un conjunto dado de objetos de datos, pero sí tiene acceso a ellos individualmente o al menos a algunos de ellos y es capaz de reunir la información a la que debería. *no* tengo acceso. El proceso de juntar la información se llama inferencia. Se pueden implementar dos tipos de medidas de acceso para ayudar a prevenir el acceso a información inferible:

- *El control de acceso dependiente del contenido* basa el acceso en la sensibilidad de los datos. Por ejemplo, un director de departamento puede tener acceso a los sueldos de los empleados de su departamento, pero no a los sueldos de los empleados de otros departamentos. El costo de esta medida es un aumento de la sobrecarga de procesamiento.
- *El control de acceso dependiente del contexto* basa el acceso a los datos en múltiples factores para ayudar a prevenir la inferencia. El control de acceso puede ser una función de factores como la ubicación, la hora del día y el historial de acceso anterior.

Vistas de base de datos

El acceso a la información en una base de datos generalmente se controla mediante el uso de vistas de la base de datos. Una vista se refiere al conjunto de datos dado que un usuario o grupo de usuarios puede ver cuando accede a la base de datos. Antes de que un usuario pueda utilizar una vista, debe tener permiso tanto en la vista como en todos los objetos dependientes. Las vistas refuerzan el concepto de privilegio mínimo.

Bloqueos de base de datos

Los bloqueos de la base de datos se utilizan cuando un usuario accede a un registro que impide que otro usuario acceda al registro al mismo tiempo para evitar ediciones hasta que el primer usuario haya terminado. El bloqueo no solo proporciona exclusividad a las escrituras, sino que también controla la lectura de modificaciones sin terminar o datos no confirmados.

Poliinstanciación

*La poliinstanciación* es un proceso que se utiliza para evitar infracciones de la inferencia de datos, como las amenazas a las bases de datos cubiertas anteriormente. Para ello, permite que una relación contenga varias tuplas con las mismas claves primarias, y cada instancia se distingue por un nivel de seguridad. Evita que los usuarios de bases de datos de bajo nivel infieran la existencia de datos de nivel superior.

Prueba OLTP ACID

Se utiliza un sistema de procesamiento de transacciones en línea (OLTP) para monitorear problemas tales como procesos que dejan de funcionar. Su objetivo principal es evitar que las transacciones que no se realizan correctamente o que no están completas entren en vigor. Una prueba ACID garantiza que cada transacción tenga las siguientes propiedades antes de que se confirme:

- **Atomicidad :** todas las operaciones están completas o los cambios en la base de datos se revierten.
- **Coherencia :** la transacción sigue un proceso de integridad que garantiza que los datos sean coherentes en todos los lugares donde existen.
- **Aislamiento :** una transacción no interactúa con otras transacciones hasta que se completa.
- **Durabilidad : una** vez que se verifica, la transacción se confirma y no se puede revertir.

Auditoría de datos

Si bien una organización puede tener implementado el plan de administración de datos más actualizado, la administración de datos por sí sola no es suficiente para protegerlos por completo. Las organizaciones también deben implementar un mecanismo de auditoría de datos que ayude a los administradores a identificar las vulnerabilidades antes de que ocurran los ataques. Los mecanismos de auditoría se pueden configurar para monitorear casi cualquier nivel de acceso a

los datos. Sin embargo, los mecanismos de auditoría afectan el desempeño de los sistemas que se auditan. Siempre considere cuidadosamente cualquier impacto en el desempeño que pueda ocurrir como resultado del mecanismo de auditoría. Si bien la auditoría es necesaria, es importante no auditar tantos eventos que los registros de auditoría estén llenos de información inútil o no utilizada.

Los datos confidenciales o sensibles deben auditarse con más cuidado que la información pública. De hecho, puede que ni siquiera sea necesario auditar el acceso a la información pública. Pero al considerar la auditoría de datos confidenciales, una organización puede decidir auditar todo el acceso a esos datos o simplemente intentar cambiar los datos. Solo la organización y su personal pueden desarrollar el mejor plan de auditoría.

Por último, la auditoría es buena solo si hay una revisión periódica de los registros producidos. Los administradores o profesionales de la seguridad deben obtener la formación adecuada sobre la revisión de registros de auditoría. Además, se deben configurar las alertas apropiadas si ocurren ciertos eventos críticos. Por ejemplo, si se bloquean varias cuentas de usuario debido a intentos de inicio de sesión no válidos durante un período corto de tiempo, esto puede ser una indicación de que los sistemas están experimentando un diccionario u otro ataque de contraseña. Si se programó una alerta para notificar a los administradores cuando ocurre una cierta cantidad de bloqueos durante un período de tiempo, los administradores pueden reducir el problema antes de que el atacante logre un acceso exitoso.

Propiedad de la información y los activos

Si bien la información y los activos dentro de una organización son en última instancia propiedad de la organización, generalmente se entiende que la información y los activos dentro de la organización son propiedad y están administrados por diferentes unidades de negocio. Estas unidades de negocio deben trabajar juntas para garantizar que se cumpla la misión de la organización y que la información y los activos estén protegidos.

Por esta razón, los profesionales de la seguridad deben comprender dónde se encuentran las diferentes informaciones y activos y trabajar con los distintos propietarios para garantizar que la información y los activos estén protegidos. Los propietarios con los que los profesionales de seguridad deben trabajar incluyen propietarios de datos, propietarios de sistemas y propietarios de empresas / misiones. Como parte de la propiedad de los activos, los profesionales de la seguridad deben asegurarse de que se desarrollen y sigan los procedimientos adecuados de gestión de activos, como se describe en el Capítulo 7 , " Operaciones de seguridad ".

Proteger la privacidad

La privacidad de los activos implica garantizar que todos los activos de la organización tengan el nivel de privacidad necesario. La privacidad es el derecho de un individuo a controlar su propia información. La privacidad se analiza en detalle en el Capítulo 1 , pero cuando se trata de la seguridad de los activos, debe comprender cómo proteger la privacidad de los activos. Esta sección analiza las responsabilidades de protección de la privacidad de los propietarios y procesadores de datos, la retención de datos y la limitación de la recopilación.

## Propietarios

Los profesionales de la seguridad deben trabajar con los propietarios de la información y los activos para determinar quién debe tener acceso a la información y los activos, el valor de la información y los activos y los controles que deben implementarse para proteger la privacidad de la información y los activos. Como resultado, los profesionales de la seguridad deben comprender el papel de los propietarios de datos, propietarios de sistemas y propietarios de empresas / misiones.

### Propietarios de datos

Como se indicó anteriormente, los propietarios de los datos son los propietarios de los datos. Desafortunadamente, en la mayoría de los casos, los propietarios de los datos no son propietarios de los sistemas en los que residen sus datos. Por lo tanto, es importante que el propietario de los datos trabaje en estrecha colaboración con el propietario del sistema. Incluso si se configuran las ACL adecuadas para los datos, los datos aún pueden verse comprometidos si el sistema en el que residen los datos no está protegido adecuadamente.

### Propietarios del sistema

Los propietarios del sistema son responsables de los sistemas en los que residen los datos. Si bien el propietario de los datos es el propietario de los datos y el custodio de los datos configura los permisos adecuados para el acceso del usuario a los datos, el propietario del sistema debe determinar los parámetros que gobiernan el sistema, como qué tipos de datos y aplicaciones se pueden almacenar en el sistema, quién posee los datos y las aplicaciones, y quién determinó los usuarios que pueden acceder a los datos y las aplicaciones.

### Custodios del sistema

Los custodios del sistema son responsables de administrar los sistemas en los que residen los datos según los parámetros establecidos por el propietario del sistema.

### Propietarios de empresas / misiones

Los propietarios de empresas o misiones deben asegurarse de que todas las operaciones se ajusten a los objetivos y la misión de la empresa. Esto incluye asegurarse de que los datos recopilados sean necesarios para que la empresa funcione. La recopilación de datos innecesarios desperdicia tiempo y recursos. Debido a que el propietario de la empresa / misión se preocupa principalmente por la empresa en general, los conflictos entre los propietarios de datos, los custodios de datos y los propietarios de sistemas pueden necesitara ser resuelto por el propietario de la empresa / misión, quien deberá tomar la mejor decisión para la organización. Por ejemplo, digamos que un propietario de datos solicita más espacio en un sistema para el almacenamiento de datos. El propietario de los datos cree firmemente que los nuevos datos que se recopilan ayudarán al equipo de ventas a ser más eficiente. Sin embargo, el almacenamiento en el activo del propietario del sistema es un bien escaso. El propietario del sistema no está dispuesto a permitir que el propietario de los datos utilice la cantidad de espacio que ha solicitado. En este

caso, el propietario de la empresa / misión tendría que revisar ambos lados y decidir si la recopilación y el almacenamiento de los nuevos datos generaría un aumento suficiente de los ingresos para justificar el costo de permitir al propietario de los datos más espacio de almacenamiento. Si es así, también puede ser necesario invertir en más medios de almacenamiento para el sistema o mover los datos a otro sistema que tenga más recursos disponibles.

Los profesionales de la seguridad siempre deben ser parte de estas decisiones porque comprenden los controles de seguridad establecidos para cualquier sistema involucrado y los controles de seguridad necesarios para proteger los datos. Mover los datos a un sistema que no tiene los controles adecuados puede causar más problemas que simplemente actualizar el sistema en el que residen los datos actualmente. Solo un profesional de la seguridad puede evaluar objetivamente las necesidades de seguridad de los datos y asegurarse de que se cumplan.

Procesadores de datos

Los procesadores de datos son cualquier personal dentro de una organización que procesa los datos que se han recopilado a lo largo de todo el ciclo de vida de los datos. Si alguna persona accede a los datos de alguna manera, esa persona puede considerarse un procesador de datos. Sin embargo, en algunas organizaciones, los procesadores de datos son solo aquellas personas que pueden ingresar o cambiar datos.

Independientemente de la definición que utilice una organización, es importante que los profesionales de seguridad trabajen para brindar capacitación a todos los procesadores de datos sobre la importancia de la privacidad de los activos, especialmente la privacidad de los datos. Esto generalmente se incluye como parte de la capacitación de concienciación sobre seguridad. También es importante incluir cualquier norma o política de privacidad que se base en leyes y regulaciones. Una vez que el personal haya recibido la capacitación adecuada, debe firmar una declaración que diga que cumplirá con la política de privacidad de la organización.

Remanencia de datos

Siempre que se borran o eliminan datos de un medio de almacenamiento, los datos residuales se pueden dejar atrás. Esto puede permitir que los datos se reconstruyan cuando la organización se deshaga de los medios, lo que da como resultado que personas o grupos no autorizados obtengan acceso a datos privados. Los medios que los profesionales de la seguridad deben considerar incluyen unidades de disco duro magnético, unidades de estado sólido, cintas magnéticas y medios ópticos, como CD y DVD.Al considerar la remanencia de datos, los profesionales de la seguridad deben comprender tres contramedidas:

- **Eliminación:** esto incluye la eliminación de datos de los medios para que los datos no se puedan reconstruir utilizando técnicas y herramientas normales de recuperación de archivos. Con este método, los datos solo se pueden recuperar mediante técnicas forenses especiales. La sobrescritura es una técnica de limpieza que escribe patrones de datos en todo el medio, eliminando así cualquier rastro de datos. Otra técnica de limpieza es la limpieza del disco.

- **Purga:** también conocida como *desinfección* , la purga hace que los datos sean ilegibles incluso con técnicas forenses avanzadas. Con esta técnica, los datos deberían ser irrecuperables. La desmagnetización, una técnica de purga, expone los medios a un poderoso campo magnético alterno, eliminando cualquier dato escrito previamente y dejando los medios en un estado magnéticamente aleatorizado (en blanco).
- **Destrucción: la** destrucción implica destruir los medios en los que residen los datos. El cifrado codifica los datos de los medios, lo que los hace ilegibles sin la clave de cifrado. La destrucción es el acto físico de destruir los medios de tal manera que no puedan ser reconstruidos. Triturar implica romper físicamente los medios en pedazos. Pulverizar implica reducir los medios a polvo. La pulpa altera químicamente el medio. Finalmente, la quema incinera los medios.

La mayoría de estas contramedidas funcionan para medios magnéticos. Sin embargo, las unidades de estado sólido presentan desafíos únicos porque no se pueden sobrescribir. La mayoría de los proveedores de unidades de estado sólido proporcionan comandos de desinfección que se pueden utilizar para borrar los datos de la unidad. Los profesionales de la seguridad deben investigar estos comandos para asegurarse de que sean efectivos. Otra opción para estas unidades es borrar la clave criptográfica. A menudo, se debe utilizar una combinación de estos métodos para garantizar completamente la eliminación de los datos.

La remanencia de datos también es una consideración cuando se usa cualquier solución basada en la nube para una organización. Los profesionales de la seguridad deben participar en la negociación de cualquier contrato con un proveedor basado en la nube para garantizar que el contrato cubra los problemas de remanencia de datos, aunque es difícil determinar si los datos se eliminan correctamente. El uso del cifrado de datos es una excelente manera de garantizar que la remanencia de los datos no sea una preocupación cuando se trata de la nube.

Limitación de colección

Para cualquier organización, existe una limitación de recopilación de datos basada en lo que se necesita. Los propietarios de sistemas y los custodios de datos deben monitorear la cantidad de espacio de almacenamiento libre para que comprendan las tendencias y puedan anticipar las necesidades futuras antes de que el espacio se vuelva crítico. Sin un seguimiento adecuado, los datos pueden crecer hasta el punto en queel rendimiento del sistema se ve afectado. Ninguna organización quiere que se apague un sistema de almacenamiento de datos vitales porque no hay espacio libre disponible. Las cuotas de disco permiten a los administradores establecer límites de espacio en disco para los usuarios y luego monitorear automáticamente el uso del espacio en disco. En la mayoría de los casos, las cuotas se pueden configurar para notificar a los usuarios cuando se acercan a los límites de espacio.

La recopilación de datos también está limitada en base a leyes y regulaciones y, en algunos casos, al obtener el consentimiento del sujeto de los datos. Las organizaciones deben asegurarse de documentar completamente las leyes y regulaciones que afectan la recopilación de datos privados y ajustar las políticas de recopilación de datos privados en consecuencia. Las organizaciones deben documentar y archivar el consentimiento del interesado. Además, este

consentimiento debe renovarse periódicamente, especialmente si la política de cobranza cambia de alguna manera.

Los profesionales de la seguridad deben trabajar con los propietarios del sistema y los custodios de datos para asegurarse de que se configuren los mecanismos de alerta y monitoreo adecuados. Los propietarios de sistemas y los custodios de datos pueden ser proactivos en lo que respecta a las necesidades de almacenamiento de datos.

Retención de activos

Los requisitos de retención de datos y activos varían en función de varios factores, incluidos el tipo de datos o activos, la antigüedad de los datos o activos y los requisitos legales y reglamentarios. Los profesionales de la seguridad deben comprender dónde se almacenan los datos y el tipo de datos almacenados. Además, los profesionales de la seguridad deben brindar orientación sobre la administración y el archivo de datos. Por lo tanto, las políticas de retención de datos deben establecerse con la ayuda del personal de la organización. Los activos que almacenan datos utilizarán las políticas de retención de datos para ayudar a guiar las pautas de retención de activos. Si es necesario reemplazar un activo de almacenamiento, es esencial una comprensión profunda de los datos que residen en el activo para garantizar que los datos se conserven durante el período requerido.

Una política de retención generalmente contiene el propósito de la política, la parte de la organización afectada por la política, las exclusiones de la política, el personal responsable de supervisar la política, el personal responsable de los datos, los tipos de datos cubiertos por la política y el calendario de retención. Los profesionales de la seguridad deben trabajar con los propietarios de los datos para desarrollar la política de retención de datos adecuada para cada tipo de datos que posee la organización. Los ejemplos de tipos de datos incluyen, entre otros, datos de recursos humanos, datos de cuentas por pagar / por cobrar, datos de ventas, datos de clientes y correo electrónico.

Los profesionales de la seguridad deben asegurarse de que también se redacten las políticas de retención de activos. Si bien las políticas de retención de activos a menudo se rigen por las políticas de retención de datos, las organizaciones pueden encontrar necesario reemplazar los activos físicos mientras necesitan retener los datos almacenados en el activo. Los profesionales de seguridad deben asegurarse de que los datos que residen en un activo que se retirará estén completamente documentados y correctamenteretenido como se detalla en la política de retención de datos. Por lo general, esto requerirá que los datos se muevan a otro activo. Por ejemplo, suponga que una organización almacena todos los datos PII que retiene en un servidor SQL ubicado en la zona desmilitarizada (DMZ) de la organización. Si la organización decide reemplazar el servidor SQL con una nueva computadora con Windows Server 2016, será necesario hacer una copia de seguridad de la PII del servidor anterior y restaurarla en el nuevo servidor. Además, es posible que la organización desee conservar la copia de seguridad de la PII y almacenarla en un lugar seguro u otro lugar seguro, en caso de que la organización alguna vez lo necesite. Luego, la organización debe asegurarse de que la PII no se pueda recuperar del disco duro del servidor anterior. Esto puede requerir la destrucción física del disco duro.

Para diseñar políticas de retención de datos y activos, la organización debe responder las siguientes preguntas:

- ¿Cuáles son los requisitos legales / reglamentarios y las necesidades comerciales para los activos / datos?
- ¿Cuáles son los tipos de activos / datos?
- ¿Cuáles son los períodos de retención y las necesidades de destrucción de los activos / datos?

El personal que esté más familiarizado con cada activo y tipo de datos debe trabajar con profesionales de seguridad para determinar las políticas de retención de activos y datos. Por ejemplo, el personal de recursos humanos debe ayudar a diseñar las políticas de retención de datos para todos los activos y datos de recursos humanos. Al diseñar políticas de retención de datos y activos, una organización debe considerar los medios y el hardware que se utilizarán para retener los datos. Luego, con esta información en la mano, la organización y / o unidad de negocios debe redactar y adoptar formalmente las políticas de retención de datos y activos.

Una vez que se han creado las políticas de retención de datos y activos, el personal debe estar capacitado para cumplir con estas políticas. La auditoría y el monitoreo deben configurarse para garantizar el cumplimiento de la política de retención de datos. Periódicamente, los propietarios y procesadores de datos deben revisar las políticas de retención de datos para determinar si es necesario realizar algún cambio. Todas las políticas de retención de datos, planes de implementación, capacitación y auditoría deben estar completamente documentadas. Además, el personal de soporte de TI debe trabajar para garantizar que los activos en los que se almacenan los datos se mantengan actualizados con los últimos parches y actualizaciones de seguridad.

Recuerde que dentro de la mayoría de las organizaciones, no es posible encontrar una solución única para todos debido a los diferentes tipos de activos o datos. Solo aquellos más familiarizados con cada activo o tipo de datos pueden determinar la mejor política de retención para ese activo o datos. Si bien un profesional de la seguridad debe participar en el diseño de las políticas de retención, el profesional de la seguridad está ahí para garantizar que siempre se considere la seguridad y que las políticas de retención satisfagan las necesidades de la organización. El profesional de la seguridad debe actuar únicamente como asesor y debe aportar su experiencia cuando sea necesario.

Controles de seguridad de datos

Ahora es el momento de discutir los controles de seguridad de datos que las organizaciones deben considerar como parte de un plan de seguridad integral. Los profesionales de la seguridad deben comprender lo siguiente como parte de los controles de seguridad de los datos: seguridad de los datos, estados de los datos (datos en reposo, datos en tránsito y datos en uso), acceso e intercambio de datos, almacenamiento y archivo de datos, líneas de base, alcance y adaptación, estándares selección y criptografía.

Seguridad de datos

La seguridad de los datos incluye los procedimientos, procesos y sistemas que protegen los datos del acceso no autorizado. El acceso no autorizado incluye el acceso físico y digital no autorizado. La seguridad de los datos también protege los datos contra cualquier amenaza que pueda afectar la confidencialidad, integridad o disponibilidad de los datos.

Para brindar seguridad a los datos, la seguridad debe implementarse utilizando una estrategia de defensa en profundidad, como se discutió en el Capítulo 1 . Si no se analiza una sola capa de acceso, la seguridad de los datos está en riesgo. Por ejemplo, puede implementar mecanismos de autenticación para asegurarse de que los usuarios deban autenticarse antes de acceder a la red. Pero si no cuenta con los controles de seguridad física adecuados para evitar el acceso no autorizado a sus instalaciones, un atacante puede acceder fácilmente a su red simplemente conectando un dispositivo no autorizado a la red.

Los profesionales de seguridad deben asegurarse de que su organización implemente medidas y salvaguardas para cualquier amenaza que haya sido identificada. Además, los profesionales de la seguridad deben permanecer atentos y estar constantemente atentos a nuevas amenazas.

Estados de datos

Se deben considerar tres estados de datos básicos como parte de la seguridad de los activos. Estos tres estados son datos en reposo, datos en tránsito y datos en uso. Los profesionales de la seguridad deben asegurarse de que se implementen controles para proteger los datos en estos tres estados.

Los datos en reposo

Los datos en reposo son datos que se almacenan y no se utilizan activamente en un momento determinado. Mientras los datos están en reposo, los profesionales de seguridad deben asegurarse de que se garantice la confidencialidad, integridad y disponibilidad de los datos. La confidencialidad se puede proporcionar implementando el cifrado de datos. La integridad se puede proporcionar mediante la implementación de los mecanismos de autenticación adecuados y las ACL de modo que solo los usuarios autorizados y autenticados puedan editar los datos. La disponibilidad se puede proporcionar implementando una solución de almacenamiento tolerante a fallas, como RAID.

Datos en tránsito

Los datos en tránsito son datos que se transmiten a través de una red. Mientras se transmiten los datos, los profesionales de la seguridad deben asegurarse de que se garantice la confidencialidad, integridad y disponibilidad de los datos. La confidencialidad se puede proporcionar mediante la implementación de cifrado de enlace o cifrado de extremo a extremo. Al igual que con los datos en reposo, la autenticación y las ACL pueden ayudar con la integridad de los datos en tránsito. La disponibilidad se puede proporcionar implementando granjas de servidores y backbones duales.

Datos en uso

Los datos en uso son datos a los que se accede o se manipula de alguna manera. La manipulación de datos incluye editar los datos y compilarlos en informes. Los principales problemas con los datos en uso son garantizar que solo las personas autorizadas tengan acceso o puedan leer los datos y que solo se permitan cambios autorizados en los datos. La confidencialidad se puede proporcionar mediante el uso de filtros de pantalla o de privacidad para evitar que personas no autorizadas lean datos en una pantalla. También se puede proporcionar mediante la implementación de una política de destrucción de documentos para todos los informes que contienen PII, PHI, datos de propiedad u otra información confidencial. La integridad de los datos se puede proporcionar implementando los controles apropiados sobre los datos. Los bloqueos de datos pueden evitar que se modifiquen los datos y las reglas de datos pueden garantizar que los cambios solo ocurran dentro de los parámetros definidos. Para ciertos tipos de datos, Las organizaciones pueden decidir implementar controles de dos personas para garantizar que los cambios en los datos se ingresen y verifiquen. La disponibilidad se puede proporcionar utilizando las mismas estrategias que se utilizan para los datos en reposo y los datos en tránsito. Además, las organizaciones pueden desear implementar bloqueos y vistas para garantizar que los usuarios que necesitan acceso a los datos obtengan la versión más actualizada de esos datos.

Acceso y uso compartido de datos

El personal debe poder acceder y compartir datos en sus tareas diarias. Este acceso comienza cuando el propietario de los datos aprueba el acceso de un usuario. El custodio de datos le otorga al usuario los permisos adecuados para los datos. Pero estos dos pasos son una simplificación excesiva del proceso. Los profesionales de seguridad deben asegurarse de que la organización comprenda cuestiones como las siguientes:

- ¿Existen las políticas de datos adecuadas para controlar el acceso y el uso de los datos?
- ¿Los propietarios de los datos comprenden las necesidades de acceso de los usuarios?
- ¿Cuáles son los diferentes niveles de acceso que necesitan los usuarios?
- ¿Qué formatos de datos necesitan los usuarios?
- ¿Hay subconjuntos de datos que solo deberían tener acceso restringido para los usuarios?
- De los datos que se recopilan, ¿hay datos privados frente a datos públicos claramente identificados?
- ¿Se protegen los datos tanto en reposo como en tránsito?
- ¿Existe algún problema legal o jurisdiccional relacionado con la ubicación de almacenamiento de datos, la transmisión de datos o el procesamiento de datos?

Si bien los propietarios y los custodios de los datos trabajan juntos para responder a muchas de estas preguntas, los profesionales de seguridad deben participar para guiarlos a través de este proceso. Si se toma la decisión de retener datos, la decisión debe basarse en la privacidad, la confidencialidad, la seguridad o las restricciones legales / reglamentarias. Los criterios por los cuales se toman estas decisiones deben registrarse como parte de una política oficial.

Almacenamiento y archivo de datos

El almacenamiento y el archivo de datos están relacionados con la forma en que una organización almacena los datos, tanto los datos digitales como los físicos en forma de copias

impresas. Es muy fácil que los datos se vuelvan obsoletos. Una vez que los datos están desactualizados, ya no son útiles para la organización.

Si bien el almacenamiento de datos solía ser bastante caro, se ha vuelto más barato en los últimos años. Los profesionales de seguridad deben trabajar con los propietarios y custodios de datos para ayudar a establecer una política de revisión de datos para garantizar que los datos se revisen periódicamente para determinar si son necesarios y útiles para la organización. Los datos deben archivarse de acuerdo con las políticas y programas de retención. Los datos que ya no son necesarios o útiles para la organización deben destruirse. La excepción son los datos que se han archivado que deben conservarse durante un período determinado en función de un período de política de retención establecido, especialmente los datos que pueden estar en retención legal.

**Nota**

La retención es un conjunto de reglas dentro de una organización que dicta los tipos de datos inalterados que deben conservarse y durante cuánto tiempo. El archivo es el proceso de almacenar de forma segura datos inalterados para su posterior recuperación potencial. Los datos deben conservarse de acuerdo con un programa documentado, almacenarse de manera segura de acuerdo con su clasificación y eliminarse de manera segura al final del período de retención.

Al considerar el almacenamiento y el archivo de datos, los profesionales de la seguridad deben asegurarse de que los diferentes aspectos del almacenamiento se analicen adecuadamente para garantizar una implementación adecuada. Esto incluye analizar el hardware y software del servidor, el mantenimiento de la base de datos, las copias de seguridad de los datos y la infraestructura de la red. Se debe comprender cada parte del rastro digital por el que viajarán los datos para que se puedan implementar las políticas y los procedimientos adecuados para garantizar la privacidad de los activos.

Los datos que aún son necesarios y útiles para la organización deben permanecer en el almacenamiento principal para que los usuarios puedan acceder fácilmente a ellos. Los datos marcados para archivar deben moverse a algún tipo de medio de respaldo o almacenamiento secundario. Las organizaciones deben determinar la forma de almacenamiento de archivos de datos que mejor se adapte a sus necesidades. Para algunas unidades de negocio enorganización, puede ser adecuado archivar los datos en cinta magnética o medios ópticos, como DVD. Con estas formas de almacenamiento, restaurar los datos del archivo puede ser un proceso laborioso. Para las unidades de negocios que necesitan una forma más fácil de acceder a los datos archivados, algún tipo de tecnología de unidad de estado sólido o de conexión en caliente puede ser una mejor manera de hacerlo.

Independientemente del medio que elija su organización para fines de archivo, los profesionales de la seguridad deben considerar los costos de los mecanismos utilizados y la seguridad del archivo. El almacenamiento de datos archivados de los que se ha realizado una copia de seguridad en un DVD en un archivador desbloqueado puede ser más conveniente para una unidad de negocio, pero no proporciona ninguna protección a los datos del DVD. En este caso, es posible que el profesional de seguridad deba trabajar con la unidad de negocios para crear un mecanismo de almacenamiento más seguro para archivos de datos. Cuando los datos son

administrados de manera centralizada por el personal de TI o del centro de datos, el personal generalmente comprende mejor los problemas de seguridad relacionados con el almacenamiento de datos y, por lo tanto, es posible que no necesite tanta orientación de los profesionales de seguridad.

## Líneas de base

Una práctica que puede simplificar el mantenimiento de la seguridad es crear e implementar imágenes estándar que se hayan protegido con líneas de base de seguridad. Una *línea de base* es un conjunto de opciones de configuración que proporciona un piso de seguridad mínima en la imagen que se implementa. Las organizaciones deben capturar líneas de base para todos los dispositivos, incluidos los dispositivos de red, las computadoras, las computadoras host y las máquinas virtuales.

Las líneas de base se pueden controlar mediante el uso de la directiva de grupo en Windows. Estas configuraciones de política se pueden realizar en la imagen y se pueden aplicar tanto a los usuarios como a las computadoras. Esta configuración se actualiza periódicamente a través de una conexión a un controlador de dominio y el usuario no puede modificarla. También es bastante común que la imagen de implementación incluya todas las actualizaciones y parches más recientes del sistema operativo.

Cuando una red hace uso de este tipo de tecnologías, los administradores han creado un entorno operativo estándar. Las ventajas de un entorno de este tipo son un comportamiento más coherente de la red y problemas de soporte más sencillos. Los análisis del sistema deben realizarse semanalmente para detectar cambios desde la línea de base.

Los profesionales de la seguridad deben ayudar a guiar a su organización a través del proceso de establecer líneas de base. Si una organización implementa líneas de base muy estrictas, proporcionará un mayor nivel de seguridad que en realidad puede ser demasiado restrictivo. Si una organización implementa una línea de base muy laxa, proporcionará un nivel más bajo de seguridad que probablemente resultará en brechas de seguridad. Los profesionales de la seguridad deben comprender el equilibrio entre proteger los activos de la organización y permitir el acceso de los usuarios, y deben trabajar para garantizar que se comprendan ambos extremos de este espectro.

## Alcance y adaptación

El alcance y la adaptación están estrechamente vinculados a las líneas de base. El alcance y la adaptación permiten a una organización limitar su enfoque para identificar y abordar los riesgos apropiados.

*El alcance* instruye a una organización sobre cómo aplicar e implementar controles de seguridad. Los controles de seguridad de referencia son los mínimos aceptables para la organización. Cuando se seleccionan los controles de seguridad en función del alcance, se debe crear documentación que incluya los controles de seguridad que se consideraron, si se adoptaron los controles de seguridad y cómo se hicieron las consideraciones.

*La personalización* permite que una organización haga coincidir más los controles de seguridad con las necesidades de la organización. Cuando se seleccionan los controles de seguridad en función de la personalización, se debe crear documentación que incluya los controles de seguridad que se consideraron, si se adoptaron los controles de seguridad y cómo se hicieron las consideraciones.

NIST SP 800-53, que se trata ampliamente en el Capítulo 1 , proporciona algunas pautas sobre la adaptación.

Selección de estándares

Dado que las organizaciones necesitan orientación sobre la protección de sus activos, los profesionales de la seguridad deben estar familiarizados con los estándares que se han establecido. Se han formado muchas organizaciones de normalización, incluido el NIST, el Departamento de Defensa de EE. UU. (DoD) y la Organización Internacional de Normalización (ISO).

**Nota**

Los estándares se tratan ampliamente en el Capítulo 1 . Para localizar información sobre un estándar NIST o ISO en particular, consulte el Índice.

La Instrucción 8510.01 del Departamento de Defensa de EE. UU. Establece un proceso de certificación y acreditación para los sistemas de información del Departamento de Defensa. Se puede encontrar en http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf .

La organización ISO trabaja con la Comisión Electrotécnica Internacional (IEC) para establecer muchos estándares relacionados con la seguridad de la información. Las normas ISO / IEC que los profesionales de la seguridad deben comprender se tratan en el Capítulo 1 .

Los profesionales de la seguridad también pueden necesitar investigar otros estándares, incluidos los estándares de la Agencia Europea de Seguridad de la Red y la Información (ENISA), la Unión Europea (UE) y la Agencia de Seguridad Nacional de EE. UU. (NSA). Es importante que la organización investigue los muchos estándares disponibles y aplique las pautas más beneficiosas según las necesidades de la organización.

Métodos de protección de datos

Los datos están protegidos de diversas formas. Los profesionales de la seguridad deben comprender los diferentes métodos de protección de datos y saber cómo implementarlos. Los métodos de protección de datos deben incluir controles administrativos (gerenciales), lógicos (técnicos) y físicos. Todos los tipos de controles se tratan ampliamente en el Capítulo 1 .

El método más popular para proteger los datos y garantizar la integridad de los datos es el uso de criptografía.

Criptografía

La criptografía, también conocida como cifrado, puede proporcionar una protección diferente según el nivel de comunicación que se esté utilizando. Los dos tipos de niveles de comunicación de cifrado son el cifrado de enlace y el cifrado de extremo a extremo.

**Nota**

La criptografía se analiza con más detalle en el Capítulo 3 , " Arquitectura e ingeniería de seguridad ".

**Cifrado de enlaces**

El cifrado de enlace cifra todos los datos que se transmiten a través de un enlace. En este tipo de comunicación, la única parte del paquete que no está encriptada es la información de control del enlace de datos, que es necesaria para garantizar que los dispositivos transmitan los datos correctamente. Toda la información está encriptada, y cada enrutador u otro dispositivo descifra la información de su encabezado para que pueda ocurrir el enrutamiento y luego se vuelve a encriptar antes de enviar la información al siguiente dispositivo.

Si la parte remitente necesita asegurarse de que la seguridad y la privacidad de los datos se mantengan a través de un enlace de comunicación público, entonces se debe utilizar el cifrado del enlace. Este es a menudo el método utilizado para proteger la comunicación por correo electrónico o cuando los bancos u otras instituciones que tienen datos confidenciales deben enviar esos datos a través de Internet.

El cifrado de enlace protege contra los rastreadores de paquetes y otras formas de escucha clandestina y se produce en el enlace de datos y las capas físicas del modelo OSI. Las ventajas del cifrado de enlaces incluyen: Todos los datos están cifrados y no es necesaria la interacción del usuario para su uso. Las desventajas del cifrado de enlace incluyen: Cada dispositivo a través del cual se deben transmitir los datos debe recibir la clave, los cambios de clave deben transmitirse a cada dispositivo en la ruta y los paquetes se descifran en cada dispositivo.

**Encriptado de fin a fin**

El cifrado de extremo a extremo cifra menos información del paquete que el cifrado de enlace. En el cifrado de extremo a extremo, la información de enrutamiento de paquetes y los encabezados y direcciones de los paquetes no están cifrados. Esto permite a los piratas informáticos potenciales obtener más información si un paquete se adquiere mediante el rastreo o la escucha clandestina de paquetes.

El cifrado de un extremo a otro tiene varias ventajas. Un usuario generalmente inicia el cifrado de extremo a extremo, lo que le permite seleccionar exactamente qué se cifra y cómo. Afecta el rendimiento de cada dispositivo a lo largo de la ruta menos que el cifrado de enlace porque no todos los dispositivos tienen que realizar cifrado / descifrado para determinar cómo enrutar el paquete.

## Requisitos de manejo de información y activos

Las organizaciones deben establecer los requisitos adecuados de manejo de información y activos para proteger sus activos. Como parte de estos requisitos de manipulación, se debe instruir al personal sobre cómo marcar, etiquetar, almacenar y destruir o desechar los medios.

Los estándares de manejo informan a los custodios y usuarios cómo proteger la información que utilizan y los sistemas con los que interactúan. Los estándares de manejo dictan por nivel de clasificación cómo se debe almacenar, transmitir, comunicar, acceder, retener y destruir la información. Los estándares de manejo pueden extenderse a la gestión de incidentes y la notificación de infracciones. Los estándares de manejo se extienden a herramientas automatizadas, como las soluciones de prevención de pérdida de datos (DLP). Los estándares de manejo deben documentarse sucintamente en un formato utilizable. Se debe hacer referencia al cumplimiento del estándar de manejo en la política de uso aceptable (AUP). Los usuarios deben conocer los estándares de manejo durante el proceso de incorporación. Los estándares de manipulación deben reforzarse a lo largo del ciclo de vida del usuario.

## Marcado, etiquetado y almacenamiento

Etiquete claramente todas las formas de medios de almacenamiento (cintas, unidades ópticas, etc.) y guárdelos de forma segura. Algunas pautas en el área de control de medios son:

- Marque con precisión y rapidez todos los medios de almacenamiento de datos.
- Asegure el almacenamiento ambiental adecuado de los medios.
- Garantizar el manejo seguro y limpio de los medios.
- Medios de registro de datos para proporcionar un control de inventario físico.

El entorno donde se almacenarán los medios también es importante. Por ejemplo, comienzan a producirse daños en los medios magnéticos por encima de los 100 grados.

El etiquetado es el vehículo para comunicar la clasificación asignada a los custodios, usuarios y aplicaciones (por ejemplo, control de acceso y DLP). Las etiquetas facilitan la identificación de la clasificación de datos. Las etiquetas pueden adoptar muchas formas: electrónicas, impresas, de audio o visuales. Las etiquetas deben ser apropiadas para la audiencia destinataria. Las etiquetas trascienden el conocimiento institucional y brindan estabilidad en entornos queexperimentar la rotación de personal. Las recomendaciones de etiquetado están vinculadas al tipo de medio. En formato electrónico, la etiqueta de clasificación debe formar parte del nombre del documento (por ejemplo, Historial de transacciones del cliente_Protegido). En documentos escritos o impresos, la etiqueta de clasificación debe tener una marca de agua clara, así como en el encabezado o pie de página del documento. Para los medios físicos, la etiqueta de clasificación debe estar claramente marcada en la caja usando palabras o símbolos.

## Destrucción

Durante la eliminación de medios, debe asegurarse de que no queden datos en los medios. El medio más confiable y seguro de eliminar datos de los medios de almacenamiento magnéticos,

como un casete de cinta magnética, es mediante la desmagnetización, que expone los medios a un potente campo magnético alterno. Elimina cualquier dato escrito previamente, dejando los medios en un estado magnéticamente aleatorizado (en blanco). Más información sobre la destrucción de medios se proporciona anteriormente en este capítulo, en la sección " Remanencia de datos " y en el Capítulo 7 .

Tareas de preparación de exámenes

Como se menciona en la sección " Acerca de la *Guía de certificación CISSP* , tercera edición " en la Introducción, tiene un par de opciones para la preparación del examen: los ejercicios aquí, Capítulo 9 , " Preparación final " y las preguntas de simulación del examen en el Examen de Pearson. Software de preparación en línea.

Revisar todos los temas clave

Revise los temas más importantes de este capítulo, señalados con el icono de Temas clave en el margen exterior de la página. La Tabla 2-1 enumera una referencia de estos temas clave y los números de página en los que se encuentra cada uno.


**Tabla 2-1** Temas clave del Capítulo 2

| Elemento de tema clave | Descripción | Número de página |
|---|---|---|
| Lista | Recomendaciones de NIST SP 800-122 para proteger eficazmente la PII | 147 |
| Lista | Clasificaciones del sector privado | 151 |
| Lista | Clasificaciones militares y gubernamentales | 152 |
| Lista | Ciclo de vida de la información | 153 |

Definir términos clave

Defina los siguientes términos clave de este capítulo y verifique sus respuestas en el glosario:

lista de control de acceso (ACL)

agregación

atomicidad

autenticación

disponibilidad

relación de base

base

llave candidata

cardinalidad

Certificación

columna o atributo

confidencialidad

consistencia

contaminación

criticidad

criptografía

criticidad de los datos

custodio de datos

procesamiento de datos

propietario de datos

procesadores de datos

purga de datos

calidad de los datos

sensibilidad de los datos

estructura de datos

almacén de datos

almacenamiento de datos

bloqueos de base de datos

vistas de la base de datos

defensa en profundidad

la licenciatura

dominio

durabilidad

EPHI

clave externa

guía

base de datos jerárquica

inferencia

activos de información

activos intangibles

integridad

Comisión Electrotécnica Internacional (IEC)

Organización Internacional de Normalización (ISO)

ISO / IEC 27000

aislamiento

Conectividad de base de datos Java (JDBC)

responsabilidad

almacenamiento conectado a la red (NAS)

Vinculación e incrustación de objetos (OLE)

Vinculación de objetos e incrustación de bases de datos (OLE DB)

programación orientada a objetos (OOP)

base de datos orientada a objetos (OODB)

base de datos relacional de objetos

Prueba OLTP ACID

sistema de procesamiento de transacciones en línea (OLTP)

Conectividad de base de datos abierta (ODBC)

información de identificación personal (PII)

política

poliinstanciación

información de salud protegida (PHI)

registro

integridad referencial

relación

base de datos relacional

remanencia

fila

esquema

sensibilidad

estándar

propietario del sistema

activos tangibles

vista

Responder preguntas de revisión

**1 .** ¿Cuál es el nivel de seguridad militar más alto?

1. Confidencial
2. Ultra secreto
3. Privado
4. Sensitivo

**2 .** ¿Quién es responsable de decidir qué usuarios tienen acceso a los datos?

1. Propietario de la empresa
2. Propietario del sistema
3. Propietario de los datos
4. Custodio de datos

**3 .** ¿Qué término se utiliza para la idoneidad de los datos para su uso?

1. Sensibilidad de los datos
2. Criticidad de los datos
3. Calidad de los datos
4. Clasificación de datos

**4 .** ¿Cuál es el nivel más alto de clasificación para los sistemas del sector privado?

1. Público
2. Sensitivo
3. Privado
4. Confidencial

**5 .** ¿Cuál es la primera fase del ciclo de vida de la información?

1. Mantener
2. Usar
3. Distribuir
4. Crear / recibir

**6 .** ¿Qué función organizacional posee un sistema y debe trabajar con otros usuarios para garantizar que los datos estén seguros?

1. Propietario de la empresa
2. Custodio de datos
3. Propietario de los datos
4. Propietario del sistema

**7 .** ¿Cuál es la última fase del ciclo de vida de la información?

1. Distribuir

2. Mantener
3. Desechar / almacenar
4. Usar

Respuestas y explicaciones

**1 . B.** Las entidades militares y gubernamentales clasifican los datos utilizando cinco niveles de clasificación principales, enumerados desde el nivel de sensibilidad más alto al más bajo:

1. Ultra secreto
2. Secreto
3. Confidencial
4. Sensible pero sin clasificar
5. Desclasificado

**2 . C.** El propietario de los datos es responsable de decidir qué usuarios tienen acceso a los datos.

**3 . C.** La calidad de los datos es la idoneidad de los datos para su uso.

**4 . D.** Los sistemas del sector privado suelen utilizar las siguientes clasificaciones, de mayor a menor:

1. Confidencial
2. Privado
3. Sensitivo
4. Público

**5 . D.** Las fases del ciclo de vida de la información son las siguientes:

1. Crear / recibir
2. Distribuir
3. Usar
4. Mantener
5. Desechar / almacenar

**6 . D.** El propietario del sistema es propietario de un sistema y debe trabajar con otros usuarios para garantizar que los datos estén seguros.

**7 . C.** Las fases del ciclo de vida de la información son las siguientes:

1. Crear / recibir
2. Distribuir
3. Usar
4. Mantener
5. Desechar / almacenar