Materiales para el instructor Capítulo 2: El cubo de destrezas de ciberseguridad

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 2:
El cubo de destrezas de ciberseguridad

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 2: Secciones y objetivos

2.1 El cubo de destrezas de ciberseguridad

Describa las tres dimensiones del cubo de McCumber.

2.2 TRÍADA DE CID

Describa los principios de confidencialidad, integridad y disponibilidad.

2.3 Estados de los datos

Diferencie los tres estados de los datos.

2.4 Contramedidas de la ciberseguridad

Compare los tipos de contramedidas de la ciberseguridad.

2.5 Marco de trabajo para la administración de seguridad de TI

Describa el modelo de ciberseguridad de ISO

2.1 El cubo de destrezas de ciberseguridad

Cisco | Networking Academy®
Mind Wide Open™

Las tres dimensiones

Los principios de seguridad

- La primera dimensión del cubo de destrezas de ciberseguridad identifica los objetivos para proteger al mundo cibernético. Los objetivos identificados en la primera dimensión son los principios básicos del mundo de la ciberseguridad.
- Estos tres principios son la confidencialidad, integridad y disponibilida
- Los principios proporcionan el enfoque y permiten al asistente ciberné priorizar las acciones en la protección del mundo cibernético.
- Utilice el acrónimo CID para recordar estos tres principios.

Estados de los datos

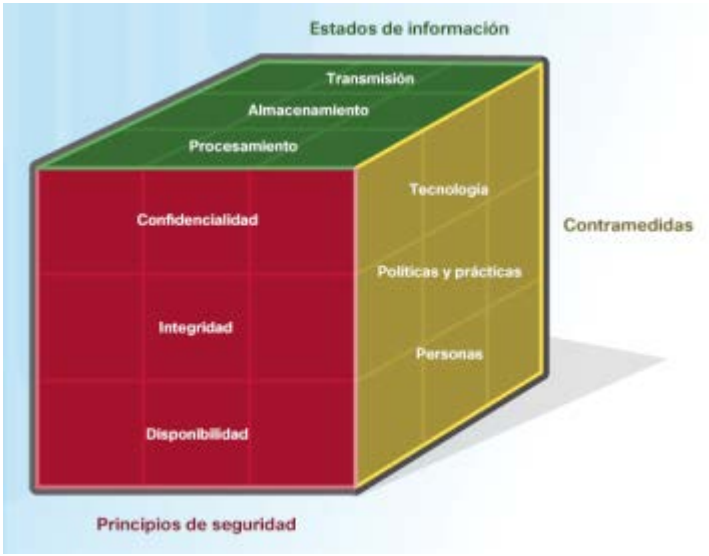
- El mundo cibernético es un mundo de datos; por lo tanto, los asistentes cibernéticos se centran en la protección de los datos. La segunda dimensión del cubo de destrezas de ciberseguridad se concentra en los problemas de proteger todos los estados de los datos en el mundo cibernético. Los datos tienen tres estados posibles:

  1) Datos almacenados 2) Datos en tránsito 3) Datos en proceso

Las tres dimensiones (cont.)

Medidas de ciberseguridad

- La tercera dimensión del cubo de destrezas de ciberseguridad define los tipos de poderes que se utilizan para proteger al mundo cibernético. El cubo de destrezas identifica los tres tipos de potencia:
- **Tecnologías:** dispositivos y productos disponibles para proteger los sistemas de información y mantener a raya a los delincuentes cibernéticos.
- **Políticas y prácticas:** procedimientos y pautas que permiten a los ciudadanos del mundo cibernético mantenerse seguros y seguir las buenas prácticas.
- **Personas:** ser consciente del mundo y de los peligros que amenazan su mundo.



2.2 TRÍADA DE CID

Cisco | Networking Academy®
Mind Wide Open™

Confidencialidad

El principio de confidencialidad

- La confidencialidad previene la divulgación de información a las personas los recursos y los procesos no autorizados. Otro término para la confidencialidad es el de privacidad.
- Las organizaciones necesitan capacitar a los empleados sobre las mejores prácticas en la protección de la información confidencial para protegerse a sí mismos y a la organización de los ataques.
- Los métodos utilizados para garantizar la confidencialidad incluyen el cifrado de datos, la autenticación y el control de acceso.

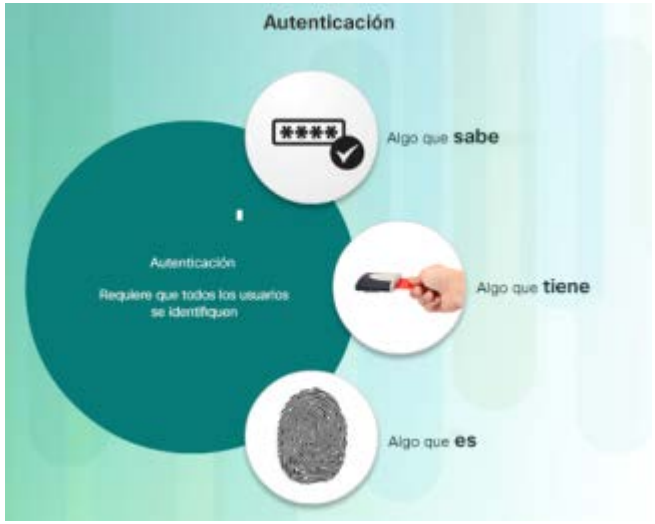
Protección de la privacidad de los datos

- Las organizaciones recolectan una gran cantidad de datos y la mayor parte de estos datos no es confidencial porque está públicamente disponible, como nombres y números de teléfono.
- Otros datos recopilados, sin embargo, son confidenciales. La información confidencial hace referencia a los datos protegidos contra el acceso no autorizado para proteger a una persona u organización.

Confidencialidad (cont.)

Control de acceso

El control de acceso define varios esquemas de protección que evita el acceso no autorizado a una computadora, red, base de datos o a otros recursos de datos. El concepto de AAA involucra tres servicios de seguridad: Autenticación, Autorización y Auditoría. ***La autenticación*** verifica la identidad de un usuario para evitar el acceso no autorizado. Los usuarios prueban su identidad con un nombre de usuario o una Id.



Los servicios autorización determinan a qué recursos pueden acceder los usuarios, junto con las operaciones que los usuarios pueden realizar. La autorización también puede controlar cuándo un usuario tiene acceso a un recurso específico.

La contabilización rastrea las actividades de los usuarios, incluidos los sitios a los que tienen acceso, la cantidad de tiempo que tienen acceso a los recursos y los cambios realizados.

Confidencialidad (cont.)

La confidencialidad y la privacidad parecen intercambiables, pero desde un punto de vista legal, tienen distintos significados.

- La mayoría de los datos de privacidad son confidenciales, pero no todos los datos confidenciales son privados. El acceso a la información confidencial ocurre después de confirmar la autorización apropiada. Las instituciones financieras, los hospitales, los profesionales médicos, los estudios jurídicos y las empresas administran la información confidencial.
- La información confidencial tiene estado privado. Mantener la confidencialidad es más que un deber ético.
- La privacidad es el uso adecuado de los datos. Cuando las organizaciones recopilan información proporcionada por los clientes o empleados, solo pueden utilizar esos datos para su objetivo previsto.

Leyes de Estados Unidos

- Ley de Privacidad de 1974
- Ley de Libertad de Información (FOIA)
- Ley de Privacidad y Registros de Educación Familiar (FERPA)
- Ley de Abuso y Fraude Informático (CFAA) de los Estados Unidos
- Ley de Protección de la Privacidad Infantil en Línea (COPPA) de los Estados Unidos
- Ley de Protección de Privacidad de Videos (VPPA)
- Ley de Portabilidad y Responsabilidad del Seguro Médico
- Ley de Gramm-Leach-Bliley (GLBA).
- Ley del Senado de California de 1386 (SB 1386)
- Reglas y normativas bancarias de Estados Unidos
- Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS)
- Ley de Informes de Crédito Justos (FCRA)

Integridad

Principio de integridad de los datos

- La integridad es la precisión, uniformidad y confiabilidad de los datos durante su ciclo de vida.
- Otro término para la integridad es el de calidad.
- Los métodos utilizados para garantizar la integridad de los datos incluyen la función de hash, las comprobaciones de validación de datos, las comprobaciones de consistencia de los datos y los controles de acceso.

La necesidad de contar con la integridad de datos

- La necesidad de contar con la integridad de datos varían según cómo una organización utiliza los datos. Por ejemplo, Facebook no verifica los datos que un usuario publica en un perfil.
- Un banco u organización financiera asigna una mayor importancia a la integridad de los datos que Facebook. Las transacciones y las cuentas de los clientes deben ser precisas.
- Proteger la integridad de los datos es un desafío constante para la mayoría de las organizaciones. La pérdida de la integridad de los datos puede lograr que todos los recursos de datos sean dudosos o inutilizables.

Verificaciones de la integridad

- Una verificación de integridad es una manera de medir la uniformidad de una recopilación de datos (un archivo, una imagen, un registro). La verificación de integridad realiza un proceso denominado función de hash para tomar una instantánea de los datos en un instante de tiempo.

Disponibilidad

La disponibilidad de los datos es el principio que se utiliza para describir la necesidad de mantener la disponibilidad de los sistemas y servicios de información en todo momento. Los ataques cibernéticos y las fallas en el sistema pueden impedir el acceso a los sistemas y servicios de información.

- Los métodos utilizados para garantizar la disponibilidad incluyen la redundancia del sistema, las copias de seguridad del sistema, mayor recuperabilidad del sistema, mantenimiento del equipo, sistemas operativos y software actualizados y planes para recuperarse rápidamente de desastres no planificados.
- Los sistemas de alta disponibilidad suelen incluir tres principios de diseño: eliminar los puntos sencillos de falla, proporcionar una conexión cruzada confiable y detectar fallas a medida que ocurren.

Las organizaciones pueden garantizar la disponibilidad al implementar lo siguiente:

1. Realizar el mantenimiento del equipo
2. Realizar actualizaciones del SO y del sistema
3. Realizar pruebas de las copias de respaldo
4. Realizar planificaciones para evitar desastres
5. Implementar nuevas tecnologías
6. Supervisar la actividad inusual
7. Realizar pruebas para verificar la disponibilidad

2.3 Estados de los datos

Cisco | Networking Academy®
Mind Wide Open™

Datos almacenados

- Los datos almacenados hacen referencia a los datos guardados. Los datos almacenados significan que un tipo de dispositivo de almacenamiento conserva los datos cuando ningún usuario o proceso los utiliza.
- Un dispositivo de almacenamiento puede ser local (en un dispositivo informático) o centralizado (en la red). Existen varias opciones para almacenar datos.
- Almacenamiento de conexión directa (DAS) proporciona almacenamiento conectado a una computadora. Una unidad de disco duro o una unidad de memoria flash USB son un ejemplo de almacenamiento de conexión directa.

Datos almacenados (cont.)

- La Matriz redundante de discos independientes (RAID) utiliza varios discos duros en una matriz, que es un método para combinar varios discos de modo que el sistema operativo los vea como un solo disco. RAID proporciona un mejor rendimiento y una mejor tolerancia a fallas.
- Un dispositivo de almacenamiento conectado a la red (NAS) es un dispositivo de almacenamiento conectado a una red que permite el almacenamiento y la recuperación de datos desde una ubicación centralizada por parte de los usuarios autorizados de la red. Los dispositivos de NAS son flexibles y escalables, lo cual significa que los administradores pueden aumentar la capacidad según sea necesario.
- Una arquitectura de red de área de almacenamiento (SAN) es un sistema de almacenamiento con base en la red. Los sistemas de SAN se conectan a la red mediante las interfaces de alta velocidad que permiten un mejor rendimiento y la capacidad para conectarse varios servidores a un repositorio centralizado de almacenamiento en disco.

Datos en tránsito

La transmisión de datos implica el envío de la información de un dispositivo a otro. Existen diversos métodos para transmitir información entre dispositivos, entre los que se incluyen los siguientes:

- **Red de transferencia**: utiliza medios extraíbles para mover físicamente los datos de una computadora a otra
- **Redes cableadas**: utilizan cables para transmitir datos
- **Redes inalámbricas**: utilizan ondas de radio para transmitir datos

La protección de los datos transmitidos es uno de los trabajos más desafiantes para un profesional de ciberseguridad. Los desafíos más grandes son los siguientes:

- **Protección de la confidencialidad de los datos**: los delincuentes cibernéticos pueden capturar, guardar y robar datos en tránsito.
- **Protección de la integridad de los datos**: los delincuentes cibernéticos pueden interceptar y alterar los datos en tránsito.
- **Protección de la disponibilidad de los datos**: los delincuentes informáticos pueden usar dispositivos falsos o no autorizados para interrumpir la disponibilidad de los datos.

Datos en proceso

El tercer estado de los datos es el de datos en proceso. Esto se refiere a los datos durante la entrada, la modificación, el cómputo o el resultado.

- La protección de la integridad de los datos comienza con la entrada inicial de datos.
- Las organizaciones utilizan varios métodos para recopilar datos, como ingreso manual de datos, formularios de análisis, cargas de archivos y datos recopilados de los sensores.
- Cada uno de estos métodos representa amenazas potenciales a la integridad de los datos.
- La modificación de los datos se refiere a cualquier cambio en los datos originales, como la modificación manual que realizan los usuarios de los datos, el procesamiento de programas y el cambio de datos, y las fallas en el equipo, lo que provoca la modificación de los datos.
- Los procesos como la codificación y decodificación, compresión y descompresión y cifrado y descifrado son ejemplos de la modificación de los datos. El código malicioso también provoca daños en los datos.

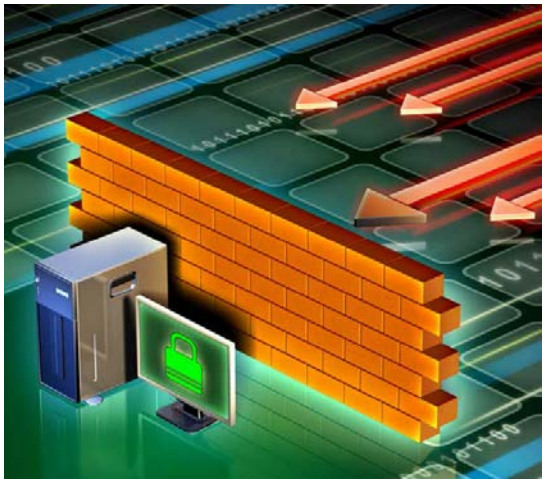
2.4 Contramedidas de la ciberseguridad

Cisco | Networking Academy®
Mind Wide Open™

Tecnologías

Medidas de protección tecnológicas con base en software

- Las medidas de protección de software incluyen programas y servicios que protegen los sistemas operativos, las bases de datos y otros servicios que operan en las estaciones de trabajo, los dispositivos portátiles y los servidores. Existen varias tecnologías basadas en software utilizadas para proteger los activos de la organización.



Medidas de protección tecnológicas con base en hardware

- Las tecnologías basadas en hardware son dispositivos que están instalados dentro de las capacidades de la red. Pueden incluir: dispositivos de firewall, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y sistemas de filtrado de contenido.

Tecnologías

Medidas de protección tecnológicas con base en la red

Las contramedidas tecnológicas también pueden incluir tecnologías con base en la red.

- **La red privada virtual (VPN)** es una red virtual segura que utiliza la red pública (es decir, Internet). La seguridad de una VPN reside en el cifrado del contenido de paquetes entre los terminales que definen la VPN.
- **Control de acceso a la red (NAC)** requiere un conjunto de verificaciones antes de permitir que un dispositivo se conecte a una red. Algunos verificaciones comunes incluyen la instalación de actualizaciones de software antivirus o de sistema operativo.
- **Seguridad de punto de acceso inalámbrico** incluye la implementación de la autenticación y encriptación.

Tecnologías

Medidas de protección tecnológicas con base en la nube

- Las contramedidas tecnológicas ahora también incluyen tecnologías con base en la nube. Las tecnologías con base en la nube cambian el componente de tecnología de la organización al proveedor de la nube.
- **Software como servicio (SaaS)** permite que los usuarios tengan acceso al software y las bases de datos de la aplicación. Los proveedores de la nube administran la infraestructura. Los usuarios almacenan datos en los servidores del proveedor de la nube.
- **Infraestructura como servicio (IaaS)** proporciona recursos informáticos virtualizados a través de Internet. El proveedor es el host del hardware, del software, de los servidores y de los componentes de almacenamiento.
- **Dispositivos de seguridad virtual** se ejecutan en un entorno virtual con un sistema operativo preempaquetado y reforzadoque se ejecuta en el hardware virtualizado.

Implementación de formación y capacitación en ciberseguridad

Un programa de reconocimiento de seguridad es sumamente importante para una organización. Un empleado puede no ser malicioso de manera intencionada, pero no conocer cuáles son los procedimientos adecuados.

Existen muchas maneras de implementar un programa de capacitación formal:

- Haga de la capacitación en el conocimiento de la seguridad una parte del proceso de incorporación de los empleados
- Vincular el conocimiento de la seguridad con los requisitos o las evaluaciones de rendimiento
- Realizar sesiones de capacitación en persona
- Completar los cursos en línea

El reconocimiento de la seguridad debe ser un proceso continuo dado que las nuevas amenazas y técnicas están siempre en el horizonte.

Políticas y procedimientos de la ciberseguridad

- Una **política** de seguridad es un conjunto de objetivos de seguridad para una empresa que incluye las reglas de comportamiento de usuarios y administradores y especificar los requisitos del sistema. Estos objetivos, estas reglas y estos requisitos en conjunto garantizan la seguridad de una red, de los datos y de los sistemas informáticos de una organización.
- **Estándares** ayudan a un personal de TI a mantener la uniformidad en el funcionamiento de la red. Los estándares proporcionan las tecnologías que los usuarios o los programas específicos necesitan, además de los requisitos o criterios del programa que una organización debe seguir.
- **Las pautas** constan de una lista de sugerencias sobre cómo hacer las cosas de manera más eficaz y segura. Son similares a los estándares, pero son más flexibles y generalmente no son obligatorias. Las pautas definen cómo se desarrollan los estándares y garantizan el cumplimiento de las políticas de seguridad general.
- **Los documentos de procedimiento** son más detallados que los estándares y las pautas. Los documentos de procedimiento incluyen detalles de implementación que contienen generalmente instrucciones paso a paso y gráficos.

2.5 Marco de trabajo para la administración de la seguridad de TI

Cisco | Networking Academy®
Mind Wide Open™

El modelo ISO

Los profesionales de seguridad necesitan proteger la información de manera completa en la organización. Esta es una tarea monumental y no es razonable esperar que una persona tenga todo el conocimiento necesario.

La **Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC)** desarrollaron un marco de trabajo global para guiar la administración de la seguridad de la información.

El modelo de ciberseguridad de ISO es para los profesionales de la ciberseguridad lo que el modelo de red de OSI es para los ingenieros de redes. Ambos proporcionan un marco para comprender y abordar las tareas complejas.

El modelo de ISO (cont.)

La norma ISO/IEC 27000 es un estándar de seguridad informática publicada en 2005 y revisada en 2013. ISO publica los estándares ISO 27000. Si bien los estándares no son obligatorios, la mayoría de los países los utilizan como marco trabajo de facto para implementar la seguridad informática.

Uso del modelo de ciberseguridad de ISO

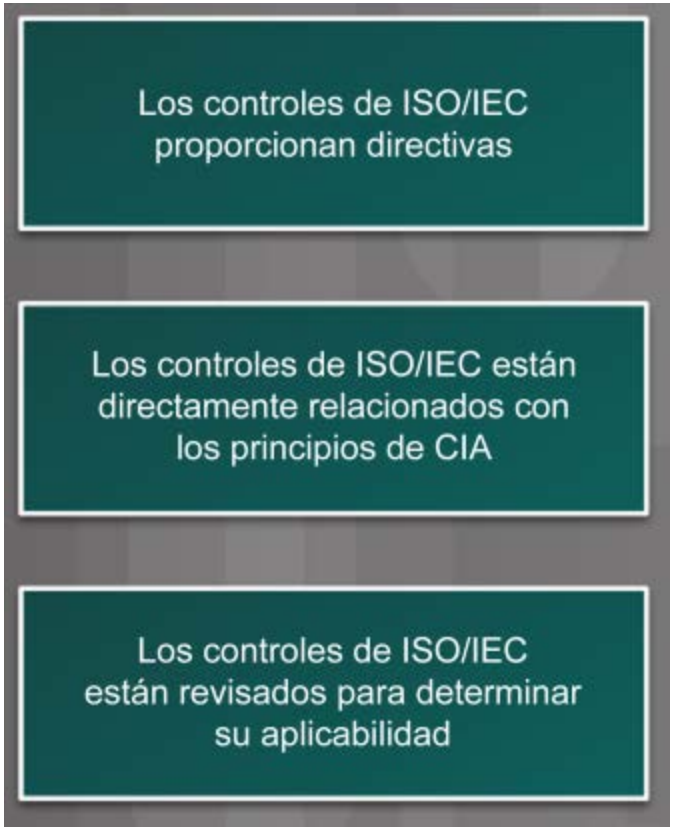
- La norma ISO 27000 es un marco de trabajo universal para cada tipo de organización. Para utilizar el marco de trabajo de manera eficaz, una organización debe restringir los dominios, los objetivos de control y los controles que aplican a su entorno y sus operaciones.
- Los objetivos de control de ISO 27001 funcionan como una lista de verificación. El primer paso que una organización toma es para determinar si estos objetivos de control se aplican a la organización.

Sección ISO/IEC 27002	Objetivo principal		
	Confidencialidad	Integridad	Disponibilidad
5			
5.1			
5.1.1	√	√	√
5.1.2	√	√	√
6			
6.1			
6.1.1	√	√	√
6.1.2		√	√
6.1.3			√
6.1.4	√		√
6.1.5	√		
6.1.6	√	√	√
6.1.7	√	√	√
6.1.8	√	√	√

Uso del modelo de ciberseguridad de ISO (cont.)

El modelo de ciberseguridad de ISO y los estados de los datos

- Los diferentes grupos de una organización pueden ser responsables de los datos de cada uno de los distintos estados.
- Por ejemplo, el grupo de seguridad de la red es responsable de los datos durante la transmisión.
- Los programadores y las personas encargadas del ingreso de los datos son responsables de los datos durante el procesamiento.
- Los especialistas en soporte de hardware y servidor son responsables de los datos almacenados. Los controles de ISO abordan específicamente los objetivos de seguridad de los datos de cada uno de los tres estados.



Uso del modelo de ciberseguridad de ISO (cont.)

El modelo y los mecanismos de protección de la ciberseguridad de ISO

- Los objetivos de control de ISO 27001 se relacionan directamente con las políticas, los procedimientos y las pautas de ciberseguridad de la organización que la administración superior determina.
- Los controles de ISO 27002 proporcionan dirección técnica. Por ejemplo, la administración superior establece una política que especifica la protección de todos los datos que ingresan o salen de la organización. La implementación de la tecnología para cumplir con los objetivos de la política no involucraría a la administración superior.
- Es responsabilidad de los profesionales de TI implementar y configurar correctamente el equipo utilizado para satisfacer las directivas de la política establecidas por la administración superior.

2.6 Resumen del capítulo

Cisco | Networking Academy®
Mind Wide Open™

Resumen

- En este capítulo se analizaron las tres dimensiones del subo de destrezas de ciberseguridad. La responsabilidad central de un asistente de ciberseguridad es proteger los sistemas y los datos de una organización.
- En el capítulo se explicó cómo cada una de las tres dimensiones contribuye a ese esfuerzo.
- En el capítulo también se analizó el modelo de ciberseguridad de ISO. El modelo representa un marco de trabajo internacional para estandarizar la administración de los sistemas de información.
- En este capítulo se analizaron los doce dominios. El modelo proporciona objetivos de control que abordan el diseño y la implementación de alto nivel de un sistema completo de administración de seguridad de la información (ISMS).
- En el capítulo también se analizó cómo los profesionales de seguridad utilizan controles para identificar las tecnologías, los dispositivos y los productos para proteger la organización.
- Si desea continuar explorando los conceptos de este capítulo, consulte la página Recursos y actividades adicionales en Recursos para el estudiante.