**Explora los dominios de seguridad del CISSP, Parte 1**

¡Hola de nuevo! Quizá recuerdes del primer curso que hay ocho dominios o categorías de seguridad identificados por el CISSP. Los equipos de seguridad los usan para organizar tareas diarias e identificar fallas de seguridad que podrían afectar negativamente a una organización, así como para definir su postura de seguridad. La postura de seguridad es la capacidad de una organización de defender sus activos y datos críticos, y reaccionar al cambio. En este video, veremos el enfoque de los primeros cuatro dominios: **seguridad y gestión de riesgos, seguridad de los activos, arquitectura y diseño de seguridad y seguridad de las comunicaciones y de las redes.**

**El primer dominio es la seguridad y gestión de riesgos.** Este dominio tiene varias áreas de enfoque: definición de metas y objetivos de seguridad, mitigación de riesgos, cumplimiento normativo, continuidad del negocio y regulaciones legales. Veamos cada área de enfoque con más detalle.

Al definir metas y objetivos de seguridad, las organizaciones pueden reducir los riesgos para activos críticos y datos como la información de identificación personal (PII). La mitigación de riesgos implica tener los procedimientos y reglas adecuados para reducir rápidamente el impacto de un riesgo como una falla de seguridad. El cumplimiento normativo es el método principal usado para desarrollar las políticas de seguridad, requisitos normativos y estándares independientes de una organización. La continuidad del negocio se relaciona con la capacidad de una organización de mantener su productividad diaria mediante el establecimiento de planes de recuperación de desastres. Finalmente, aunque las leyes de seguridad y gestión de riesgos varían en todo el mundo, sus objetivos generales son similares. Como profesional de seguridad, debes seguir las reglas y expectativas de comportamiento ético para minimizar la negligencia, el abuso o el fraude.

**El siguiente dominio es la seguridad de los activos.** Este se centra en asegurar los activos digitales y físicos. También se relaciona con almacenar, mantener, conservar y destruir datos. Esto exige que los activos como PII o SPII (información personal sensible) sean manejados y protegidos de forma segura, ya sea que se almacenen digitalmente se transfieran por una red como Internet, o que incluso se recopilen físicamente. Las organizaciones deben tener políticas y procedimientos que garanticen que los datos se almacenen, mantengan, conserven y destruyan correctamente. Saber qué datos hay y quién accede a ellos es necesario para tener una fuerte postura de seguridad que mitigue los riesgos contra los activos críticos y los datos. Antes vimos algunos ejemplos sobre la eliminación de datos. Por ejemplo, una organización puede pedirte, como analista de seguridad, supervisar la destrucción de discos duros para eliminarlos correctamente. Esto garantiza que los agentes de amenazas no accedan a los datos privados en esas unidades.

**El tercer dominio es la arquitectura y diseño de seguridad.** Este se centra en optimizar la seguridad de los datos garantizando que haya herramientas, sistemas y procesos efectivos para proteger los activos y datos de una organización. Un concepto básico de la arquitectura y diseño seguro es la responsabilidad compartida. La responsabilidad compartida es que todos dentro de una organización actúen activamente para reducir riesgos y preservar la seguridad física y virtual.

Al tener políticas que incentiven a reconocer y reportar problemas de seguridad, muchas cuestiones pueden solucionarse de forma rápida y efectiva.

**El cuarto dominio es la seguridad de las comunicaciones y de las redes.** Se centra en gestionar y proteger las redes y comunicaciones inalámbricas. Las redes seguras protegen los datos y comunicaciones de una organización, ya sea de forma física o en la nube, o al conectarse a los servicios de forma remota. Por ejemplo, las personas que trabajan en espacios públicos deben protegerse contra posibles vulnerabilidades al usar conexiones Bluetooth o redes Wi-Fi públicas inseguras. Si el equipo de seguridad elimina el acceso a esos canales de comunicación a nivel organizacional, puede que los empleados decidan evitar comportamientos inseguros que podrían aprovechar los agentes de amenazas. Después de ver el enfoque de los cuatro primeros dominios, analicemos los últimos cuatro dominios.

**Explora los dominios de seguridad del CISSP, Parte 2**

En este video, veremos los últimos cuatro dominios. **Gestión de identidades y accesos, evaluación y pruebas de seguridad, operaciones de seguridad y seguridad en el desarrollo de software.**

**El quinto dominio es la gestión de identidad y acceso (IAM).** Se centra en el acceso y autorización para proteger los datos, asegurándose de que los/las usuarios/as sigan las políticas de control y manejo de activos. Como analista de nivel inicial, es esencial mantener los sistemas y datos de una empresa lo más seguros posible, limitando el acceso a lo que los/las empleados/as necesitan. Básicamente, la IAM reduce el riesgo general para los sistemas y datos. Por ejemplo, si toda la empresa utiliza el mismo inicio de sesión de administrador, no hay forma de rastrear quién tiene acceso a qué datos. En caso de una falla de seguridad, sería imposible separar la actividad de usuario válida de la de los agentes de amenaza.

**La IAM tiene cuatro componentes principales.**

**La identificación** es cuando alguien verifica quién es brindando un nombre de usuario, una tarjeta de acceso o datos biométricos, como una huella dactilar.

**La autenticación** es el proceso de verificar la identidad de alguien mediante una contraseña o pin, por ejemplo. La autorización se da tras confirmar la identidad del usuario y su nivel de acceso, que depende del puesto en la organización.

**La responsabilidad** se refiere al monitoreo y registro de las acciones de los/las usuarios/as, como inicios de sesión, para demostrar que los sistemas y datos se utilizan adecuadamente.

**El sexto dominio de seguridad es la evaluación y pruebas de seguridad.** Este dominio se centra en realizar pruebas de control de seguridad, recopilar y analizar datos y realizar auditorías de seguridad para monitorear riesgos, amenazas y vulnerabilidades. Con las pruebas de control de seguridad se identifican formas nuevas y mejores de mitigar amenazas, riesgos y vulnerabilidades. Esto implica examinar metas y objetivos organizacionales, y evaluar si realmente se usan los controles para lograr esos objetivos. Recopilar y analizar datos de seguridad con frecuencia también ayuda a evitar amenazas y riesgos. Los/las analistas pueden usar los informes de pruebas y evaluaciones de seguridad para mejorar los controles o implementar nuevos. Un ejemplo de implementar un nuevo control es exigir usar la autenticación de varios factores para protegerse mejor contra amenazas y riesgos.

**Operaciones de seguridad**. Este dominio se centra en realizar investigaciones e implementar medidas preventivas. Las investigaciones empiezan tras identificar un incidente de seguridad. Este proceso requiere una mayor urgencia para minimizar los riesgos potenciales contra la organización. Si hay un ataque activo, es esencial mitigarlo y evitar que se intensifique para proteger la información privada contra los agentes de amenaza. Tras neutralizar la amenaza, se empezará a recopilar evidencia de datos digitales y físicos para llevar a cabo una investigación forense. Se debe realizar una investigación forense digital para identificar cuándo, cómo y por qué se produjo la falla. Con esto los equipos de seguridad definen áreas de mejora y medidas preventivas para mitigar futuros ataques.

El octavo y último dominio de seguridad es **la seguridad en el desarrollo de software.** Se centra en usar prácticas de codificación seguras. Quizá recuerdes que las prácticas de codificación seguras son pautas recomendadas para crear aplicaciones y servicios seguros.

El ciclo de vida de desarrollo de software es un proceso eficiente usado para crear rápidamente productos y funciones de software. En este proceso, la seguridad es un paso adicional. Al someter cada fase del ciclo de vida del desarrollo de software a revisiones de seguridad, la seguridad se integra por completo en el producto. Por ejemplo, realizar una revisión de diseño seguro durante la fase de diseño, revisiones de código seguro durante las fases de desarrollo y prueba y pruebas de penetración durante la fase de implementación y despliegue aseguran que la seguridad se integre en el producto de software en cada paso. Esto mantiene el software seguro y protege los datos confidenciales, y mitiga riesgos innecesarios para una organización. Conocer estos dominios puede ayudarte a comprender mejor cómo se utilizan para mejorar la seguridad general de una organización y el papel crítico que desempeña el equipo de seguridad. A continuación, veremos las amenazas, riesgos y vulnerabilidades de seguridad, incluido el ransomware, y te presentaremos las tres capas de la web.

**Dominios de seguridad que deben conocer las/los analistas de ciberseguridad**

Como analista, puedes explorar varias áreas de ciberseguridad que te interesen. Una forma de hacerlo es mediante la comprensión de los diferentes dominios de seguridad y cómo se utilizan para organizar el trabajo de las y los profesionales de la ciberseguridad. En esta lectura, aprenderás más sobre los ocho dominios de seguridad del CISSP y cómo se relacionan con el trabajo que realizarás como analista.

Gráfico de los ocho íconos que representan los dominios de seguridad del CISSP.

**Dominio 1: Seguridad y gestión de riesgos**

Todas las organizaciones deben desarrollar su postura de seguridad, es decir, su capacidad para gestionar la defensa de sus activos y datos críticos así como para reaccionar frente a los cambios. Algunos de los elementos del dominio de seguridad y gestión de riesgos que impactan en la postura de seguridad de una organización son:

Metas y objetivos de seguridad.

Procesos de mitigación de riesgos.

Cumplimiento normativo (compliance).

Planes para la continuidad del negocio.

Normativa.

Ética profesional y organizacional.

La seguridad de la información, o InfoSec, también está relacionada con este dominio y se refiere a un conjunto de procesos establecidos para proteger la información. Una organización puede usar guías o manuales de estrategias (o procedimientos) e implementar la formación como parte de su programa de seguridad y gestión de riesgos, en función de sus necesidades y de los riesgos percibidos. Existen muchos procesos de diseño de InfoSec, como:

Respuesta a incidencias.

Gestión de las vulnerabilidades.

Seguridad en la aplicación.

Seguridad en la nube.

Seguridad de la infraestructura.

Por ejemplo, un equipo de seguridad puede tener que modificar el tratamiento de la información de identificación personal (PII) para cumplir el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

**Dominio 2: Seguridad de los activos**

La seguridad de los activos implica gestionar los procesos de ciberseguridad de los activos organizacionales, lo cual incluye almacenamiento, mantenimiento, conservación y destrucción de datos físicos y virtuales. Dado que la pérdida o el robo de activos puede exponer a una compañía y aumentar el nivel de riesgo, es esencial hacer un seguimiento de los activos y los datos que contienen. Realizar un análisis del impacto en la seguridad, establecer un plan de recuperación y gestionar la exposición de los datos dependerá del nivel de riesgo asociado a cada activo. Las/los analistas de seguridad pueden necesitar almacenar, mantener y conservar datos mediante la creación de copias de seguridad, para asegurarse de poder restaurar el entorno en caso de que un incidente de seguridad ponga en riesgo los datos de la organización.

**Dominio 3: Arquitectura y diseño de seguridad**

Este dominio se enfoca en la gestión de la seguridad de los datos. Garantizar la existencia de herramientas, sistemas y procesos eficaces ayuda a proteger los activos y datos de una organización. Estos procesos son creados por quienes se dedican a la arquitectura e ingeniería de seguridad.

Un aspecto importante de este dominio es el concepto de responsabilidad compartida, que implica que todas las personas involucradas asuman un papel activo en la reducción del riesgo durante el diseño de un sistema de seguridad. Los principios de diseño adicionales relacionados con este dominio, que se tratarán más adelante en el programa, son:

Simulación de amenazas.

Principio de privilegio mínimo.

Defensa en profundidad.

Fallar de forma segura.

Separación de funciones.

Simplicidad.

Confianza cero.

Confianza tras verificación.

Un ejemplo de administración de datos es el uso de una herramienta de gestión de eventos e información de seguridad (SIEM) para monitorear los indicadores relacionados, ante un inicio de sesión o una actividad de usuario inusuales, que podrían indicar que un agente de amenaza está intentando acceder a datos privados.

**Dominio 4: Seguridad de las comunicaciones y de redes**

Este dominio se centra en la gestión y la seguridad de las redes físicas y las comunicaciones inalámbricas, incluidas las que son en el mismo lugar, remotas y en la nube.

Las organizaciones que cuentan con entornos de trabajo remotos, híbridos y presenciales (en el lugar) deben asegurarse de que los datos permanezcan seguros y, a la vez, gestionar las conexiones externas y garantizar que quienes trabajan a distancia accedan de forma segura a las redes. Diseñar controles de seguridad de red, como el acceso restringido, puede ayudar a proteger a los/las usuarios/as y garantizar que la red de una empresa permanezca segura cuando sus empleados/as viajan o trabajan fuera de la oficina principal.

**Dominio 5: Gestión de identidades y accesos**

El dominio de gestión de identidades y accesos (IAM) se centra en mantener la seguridad de los datos, asegurándose de que las identidades de los/las usuarios/as sean confiables y estén autenticadas, y que el acceso a los activos físicos y lógicos esté autorizado. Esto ayuda a prevenir el acceso de usuarios/as no autorizados/as, al tiempo que permite que quienes están autorizados/as realicen sus tareas.

Básicamente, el IAM utiliza lo que se conoce como el principio de privilegio mínimo, que es el concepto de otorgar solo el acceso y la autorización mínimos necesarios para completar una tarea. Por ejemplo, a un/a analista de ciberseguridad se le puede pedir que se asegure de que las/los representantes del servicio de atención al cliente solo puedan ver los datos privados de un/a cliente, como su número de teléfono, mientras trabajan en la resolución de un problema. Una vez resuelto el inconveniente, se deberá eliminar el acceso.

**Dominio 6: Evaluación y pruebas de seguridad**

El dominio de evaluación y pruebas de seguridad se enfoca en identificar y mitigar riesgos, amenazas y vulnerabilidades. Las evaluaciones de seguridad ayudan a las empresas a determinar si sus sistemas internos son seguros o están en riesgo. Las organizaciones pueden emplear pruebas de penetración, un proceso conocido como pentesting, para encontrar vulnerabilidades que podría aprovechar un agente de amenaza.

Este dominio sugiere que las organizaciones realicen pruebas de control de la seguridad, y que recopilen y analicen datos. Además, se enfatiza la importancia de realizar auditorías de seguridad para monitorear y reducir la probabilidad de que se produzca una filtración de datos. Para contribuir a este tipo de tareas, las y los profesionales de la ciberseguridad pueden encargarse de auditar los permisos de usuarios/as, a fin de confirmar si tienen los niveles correctos de acceso a los sistemas internos.

**Dominio 7: Operaciones de seguridad**

El dominio de operaciones de seguridad se centra en la investigación de una posible filtración de datos y la implementación de medidas preventivas después de que se haya producido un incidente. Esto incluye el uso de estrategias, procesos y herramientas como:

Entrenamiento y concientización.

Informes y documentación.

Detección y prevención de intrusiones.

Herramientas SIEM.

Gestión de registros.

Gestión de incidentes.

Manuales de estrategias (playbooks).

Análisis forense posterior a una filtración.

Reflexión sobre las lecciones aprendidas.

Los y las profesionales de ciberseguridad involucrados/as en este dominio trabajan en equipo para gestionar, prevenir e investigar amenazas, riesgos y vulnerabilidades. Están entrenados/as para hacer frente a ataques activos, como el acceso a grandes cantidades de datos desde la red interna de una organización, fuera del horario normal de trabajo. Una vez identificada una amenaza, el equipo trabaja para mantener a salvo los datos y la información privada.

**Dominio 8: Seguridad en el desarrollo de software**

El dominio de seguridad en el desarrollo de software se enfoca en el uso de prácticas y políticas de programación para crear aplicaciones seguras. Contar con ellas ayuda a ofrecer servicios seguros y fiables, y a proteger a las organizaciones y sus usuarios/as.

La seguridad debe incorporarse en cada elemento del ciclo de vida del desarrollo de software, desde el diseño y el desarrollo hasta las pruebas y el lanzamiento. Para lograr la seguridad efectiva, es necesario tener en mente la seguridad en cada paso del proceso de desarrollo de software. No se la puede considerar como un aspecto secundario o posterior.

Realizar pruebas de seguridad de las aplicaciones puede ayudar a garantizar que las vulnerabilidades sean identificadas y mitigadas adecuadamente. Además, es necesario disponer de un sistema que permita evaluar las convenciones de programación, los ejecutables de software y las medidas de seguridad incorporadas en el mismo. También, es clave contar con profesionales de control de calidad y de pruebas de penetración que se encarguen de verificar que el software cumpla con los estándares de seguridad y rendimiento establecidos. Por ejemplo, un/a analista de nivel inicial que trabaje para una empresa farmacéutica podría tener la responsabilidad de asegurarse de que el cifrado, o encriptación, esté configurado correctamente en un nuevo dispositivo médico que almacenará datos privados de pacientes.

Conclusiones clave

En esta lectura, profundizaste tus conocimientos en las áreas de enfoque de los ocho dominios de seguridad del CISSP. Además, obtuviste información sobre InfoSec y el principio del mínimo privilegio. Familiarizarte con estos dominios de seguridad y conceptos relacionados te ayudará a obtener una perspectiva en el campo de la ciberseguridad.

**Amenazas, riesgos y vulnerabilidades**

Como analista de seguridad de nivel inicial, entre otras cosas, te encargarás de manejar los activos físicos y digitales. Recuerda, un activo es un elemento percibido como teniendo valor para una organización.

Durante su vida útil, las organizaciones adquieren todo tipo de activos, incluyendo espacios de oficina, computadoras, PII de clientes, propiedad intelectual, como patentes o datos de derechos de autor, y mucho más. Lamentablemente, las organizaciones o peran en un entorno que presenta varias amenazas, riesgos y vulnerabilidades contra sus activos. Repasemos qué son las amenazas, los riesgos y las vulnerabilidades, y veamos algunos ejemplos comunes. Una amenaza es una circunstancia o evento que puede afectar negativamente a los activos. Un ejemplo de amenaza es un ataque de ingeniería social. Es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso u objetos de valor. Un método de esta amenaza es enviar correos con enlaces maliciosos que parecen provenir de empresas legítimas o de personas. Se llama phishing. Recuerda que el phishing es una técnica usada para adquirir datos sensibles, como nombres de usuario, contraseñas, o información bancaria. Los riesgos son diferentes. Un riesgo es algo que puede afectar a la confidencialidad, integridad o disponibilidad de un activo. Piensa en un riesgo como la probabilidad de que ocurra una amenaza. Un ejemplo de un riesgo para una organización podría ser la falta de protocolos de respaldo para asegurarse de que su información almacenada pueda recuperarse en caso de un accidente o incidente de seguridad. Las organizaciones califican los riesgos en diferentes niveles: bajo, medio y alto, según la probabilidad de amenaza y el valor de un activo. Un activo de bajo riesgo es información que no daña la reputación u operaciones en curso, y no causa daños financieros si se ve comprometida. Esto incluye información pública como datos en el sitio web o investigaciones publicadas. Un activo de riesgo medio es información no disponible al público que puede causar cierto daño a las finanzas, reputación u operaciones de la organización. Por ejemplo, revelar anticipadamente las ganancias trimestrales puede influir en el valor en la bolsa. Un activo de alto riesgo es información protegida por normas o leyes que, si se ve comprometida, tendría un impacto negativo grave en las finanzas, operaciones o reputación de la organización. Esto podría incluir activos filtrados con SPII, PII o propiedad intelectual.

Ahora, hablemos de las vulnerabilidades.

Una vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza. Cabe señalar que debe haber una vulnerabilidad y una amenaza para que haya un riesgo.

Ejemplos de vulnerabilidades: firewall, aplicaciones o software desactualizados; contraseñas débiles, así como datos confidenciales desprotegidos. Las personas también pueden ser consideradas una vulnerabilidad. Sus acciones pueden afectar significativamente a la red interna. Ya sean clientes, proveedores externos o empleados, mantener la seguridad debe ser un esfuerzo conjunto.

Los/las analistas de nivel inicial deben capacitar a la gente para que sea más consciente de la seguridad. Por ejemplo, enseñar a identificar un correo de phishing es un buen inicio. Usar tarjetas de acceso para dar a los/las empleados/las acceso a espacios físicos mientras se restringe a visitantes externos es otra buena medida de seguridad. Las organizaciones deben mejorar siempre sus esfuerzos para identificar y mitigar vulnerabilidades y minimizar las amenazas y riesgos. Los/las analistas de nivel inicial pueden respaldar este objetivo al fomentar que los/las empleados/as informen actividades sospechosas, así como monitorear y documentar el acceso de empleados/as a activos críticos. Ahora que conoces algunas amenazas, riesgos y vulnerabilidades que enfrentan los/las analistas, veremos a continuación su impacto en las operaciones comerciales.

**Principales repercusiones de las amenazas, riesgos y vulnerabilidades**

En este video, veremos un tipo de malware costoso llamado ransomware. Luego veremos tres impactos clave de amenazas, riesgos y vulnerabilidades en las operaciones organizacionales. El ransomware es un ataque malicioso en que los agentes de amenazas encriptan los datos de una organización y exigen un pago para restaurar el acceso. Cuando el atacante despliega el ransomware, puede trabar los sistemas de red, dejar los dispositivos inutilizables y encriptar o bloquear datos confidenciales, bloqueando así el acceso a los dispositivos. Luego, el agente de amenaza pide un rescate antes de dar una clave de descifrado para permitir que las organizaciones vuelvan a sus operaciones comerciales normales. Piensa en una clave de descifrado como una contraseña proporcionada para recuperar el acceso a tus datos. Las negociaciones de rescate o la filtración de datos por agentes de amenazas pueden ocurrir en la dark web. Mucha gente usa buscadores para ir a redes sociales o hacer compras en línea. Esto es solo un fragmento de la web. La web es una red interconectada de contenido en línea que consiste en tres capas: la web superficial, la deep web y la dark web. La web superficial es la capa que usa la mayoría. Tiene contenido accesible desde un navegador web. La deep web suele requerir autorización para acceder a ella. La intranet de una organización es un ejemplo de deep web, pues solo pueden acceder a ella colaboradores o personas autorizadas. Por último, a la dark web solo se puede acceder mediante un software especial. Generalmente tiene una connotación negativa, ya que es la preferida por los criminales debido al secretismo que proporciona. Analicemos tres impactos clave de amenazas, riesgos y vulnerabilidades. El primero es el impacto financiero. Cuando los activos se ven comprometidos por un ataque, como por el uso de malware, las consecuencias financieras pueden ser significativas por varias razones. Estas pueden incluir interrupción de la producción y los servicios, el costo para solucionar el problema y multas si los activos se ven comprometidos por un incumplimiento de las leyes y regulaciones. El segundo impacto es el robo de identidad. Las organizaciones deben decidir si almacenan datos privados de clientes, empleados/as y proveedores externos, y durante cuánto tiempo. Almacenar todo tipo de datos sensibles es un riesgo para la organización. Los datos sensibles pueden incluir información de identificación personal (PII), que puede ser vendida o filtrada a través de la dark web. Esto ocurre porque la dark web ofrece una sensación de secretismo y los agentes de amenaza venden datos ahí sin consecuencias legales. El último impacto es el daño a la reputación de una organización. Una sólida base de clientes apoya la misión de la organización, su visión y sus objetivos financieros. Si se aprovecha una vulnerabilidad, los/las clientes pueden buscar nuevas relaciones comerciales con competidores o crear mala publicidad que daña la reputación de la organización. Perder datos de clientes no solo afecta a la reputación de la organización y sus finanzas, sino que también puede generar sanciones y multas. Se recomienda que las organizaciones tomen las medidas de seguridad adecuadas y sigan ciertos protocolos para prevenir el impacto significativo de las amenazas, riesgos y vulnerabilidades. Al usar todas sus herramientas, los equipos de seguridad están mejor preparados para manejar eventos como un ransomware. A continuación, veremos los siete pasos para gestionar el riesgo del Marco de Gestión de Riesgos del NIST.

**Gestiona amenazas, riesgos y vulnerabilidades**

**Marco de Gestión de Riesgos (RMF) del NIST**

Como vimos antes, el Instituto Nacional de Estándares y Tecnología (NIST) ofrece muchos marcos utilizados por profesionales de seguridad para manejar riesgos, amenazas y vulnerabilidades. En este video, nos centraremos en el Marco de Gestión de Riesgos (RMF) del NIST. Como analista de nivel inicial, es posible que no participes en todos estos pasos, pero es importante conocer este marco.

Tener una comprensión sólida de cómo mitigar y manejar los riesgos puede diferenciarte de otros candidatos cuando comiences tu búsqueda de empleo en el campo de la seguridad. El RMF tiene siete pasos: Preparar, categorizar, seleccionar, implementar, evaluar, autorizar y monitorear. Empecemos con el primer paso: preparar. Este se refiere a las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que ocurra una falla de seguridad. Como analista de nivel inicial, puede que uses este paso para monitorear los riesgos e identificar controles que puedan utilizarse para reducirlos. El segundo paso es categorizar. Sirve para desarrollar procesos y tareas de manejo de riesgos. Los profesionales de seguridad usan esos procesos y desarrollan tareas pensando en cómo la confidencialidad, integridad y disponibilidad de los sistemas e información pueden verse afectadas. Como analista de nivel inicial, deberás entender cómo seguir los procesos establecidos por tu organización para reducir los riesgos contra activos críticos, como la información privada de clientes. El tercer paso es seleccionar. Se refiere a elegir, personalizar y capturar la documentación de los controles que protegen a una organización. Un ejemplo de seleccionar sería actualizar un manual de procedimientos o gestionar otra documentación que te permita a ti y al equipo abordar problemas de forma más eficiente. El cuarto paso consiste en implementar planes de seguridad y privacidad para la organización. Tener buenos planes es esencial para minimizar el impacto de riesgos de seguridad continuos. Por ejemplo, si notas un patrón de empleados/as que constantemente necesitan restablecer sus contraseñas, implementar un cambio en los requisitos de contraseña para resolver este problema. El quinto paso es evaluar. Se refiere a determinar si los controles establecidos se implementaron correctamente. La organización siempre quiere operar con la máxima eficiencia posible. Por eso, es esencial tomarse el tiempo para analizar si los protocolos, procedimientos y controles que se implementaron cumplen con las necesidades de la organización. En este paso, los/las analistas identifican posibles debilidades y determinan si las herramientas, procedimientos, controles y protocolos de la organización deben cambiarse para gestionar mejor los riesgos. El sexto paso es autorizar. Significa ser responsable de los riesgos de seguridad y privacidad que pueden existir en una organización. Como analista, este paso podría implicar generar informes, desarrollar planes de acción y establecer hitos del proyecto que estén alineados con los objetivos de seguridad de tu organización. El séptimo paso es monitorear.

Significa estar al tanto de cómo operan los sistemas. Evaluar y mantener las operaciones técnicas son tareas diarias de los/las analistas. Parte de mantener un nivel bajo de riesgo para una organización es saber cómo los sistemas actuales apoyan objetivos de seguridad de la organización. Si los sistemas no satisfacen los objetivos, pueden necesitarse cambios. Aunque tú no te encargues de establecer los procedimientos, deberás asegurarte de que funcionen como deben a fin de minimizar los riesgos para la organización y sus usuarios/as.

**Gestiona amenazas, riesgos y vulnerabilidades comunes**

Anteriormente, aprendiste que la ciberseguridad implica proteger a las organizaciones y a las personas de amenazas, riesgos y vulnerabilidades. Comprender el panorama actual brinda a las organizaciones la posibilidad de diseñar políticas y procesos que ayuden a prevenir y mitigar este tipo de problemas de seguridad. En esta lectura, explorarás más a fondo cómo gestionar el riesgo y algunas tácticas y técnicas comunes utilizadas por agentes de amenaza, a fin de prepararte mejor para proteger a las organizaciones y a las personas cuando ingreses al campo de la ciberseguridad.

Gestión del riesgo

Un objetivo primordial de las empresas es proteger sus activos. Un activo es un elemento que se percibe como valioso para una organización. Este puede ser digital o físico. Ejemplos de activos digitales son la información personal de colaboradores/as, clientes o proveedores, como:

Números de la Seguridad Social (SSN) o números únicos de identificación nacional asignados a personas.

Fechas de nacimiento.

Números de cuentas bancarias.

Direcciones postales.

Ejemplos de activos físicos incluyen:

Terminales de pago.

Servidores.

Computadoras de escritorio.

Espacios de oficina.

Algunas estrategias habituales utilizadas para gestionar los riesgos son:

Aceptación: aceptar un riesgo para evitar interrumpir la continuidad del negocio.

Prevención: crear un plan para evitar el riesgo por completo.

Transferencia: transferir el riesgo a un tercero para que lo gestione.

Mitigación: disminuir el impacto de un riesgo conocido.

Además, las organizaciones aplican procesos de gestión de riesgos basados en marcos ampliamente aceptados para ayudar a proteger los activos digitales y físicos frente a diversas amenazas, riesgos y vulnerabilidades. Algunos ejemplos de estos son el Marco de Gestión de Riesgos (

RMF

) del Instituto Nacional de Estándares y Tecnología (

NIST

) y la Health Information Trust Alliance (

HITRUST

).

A continuación se indican algunos tipos comunes de amenazas, riesgos y vulnerabilidades que ayudarás a gestionar a las organizaciones desde tu rol como profesional de la ciberseguridad.

**Amenazas, riesgos y vulnerabilidades más comunes**

**Amenazas**

Una amenaza es cualquier circunstancia o evento que puede afectar negativamente a los activos. Como analista de ciberseguridad de nivel inicial, tu trabajo consiste en ayudar a preservar los activos de la organización frente a amenazas internas y externas. Por lo tanto, comprender cuáles son los tipos más comunes de amenazas es importante para tu trabajo. Las amenazas comunes incluyen:

Amenazas internas: cuando miembros del personal o proveedores abusan de su acceso autorizado para obtener datos que pueden perjudicar a una organización.

Amenazas persistentes avanzadas (APT): cuando agentes de amenaza mantienen el acceso no autorizado a un sistema durante un periodo prolongado de tiempo.

Riesgos

Un riesgo es todo aquello que puede afectar la confidencialidad, integridad o disponibilidad de un activo. Una fórmula básica para determinar el nivel de riesgo es que este es igual a la probabilidad de una amenaza. Una forma de verlo es que un riesgo es llegar tarde al trabajo y las amenazas son el tráfico o un accidente que puedan ocasionar esa demora.

Existen diferentes factores que pueden afectar a la probabilidad de que se produzca un riesgo para los activos de una organización, entre ellos:

Riesgo externo: se refiere a cualquier elemento, grupo o personas fuera de la organización que tienen el potencial de dañar sus activos, como agentes de amenaza que intentan acceder a información privada.

Riesgo interno: se trata de colaboradores/as, proveedores externos o socios de confianza actuales o antiguos/as que pueden suponer un riesgo para la seguridad.

Sistemas heredados: son sistemas antiguos que, si bien pueden no estar contabilizados o actualizados, aún pueden afectar a los activos, como estaciones de trabajo o sistemas de mainframe antiguos. Por ejemplo, una organización puede tener una máquina expendedora que acepta pagos con tarjeta de crédito o una estación de trabajo que todavía está conectada al sistema de contabilidad heredado.

Riesgo de múltiples partes: hace referencia a que, el externalizar el trabajo a terceros, puede implicar darles acceso a propiedad intelectual, como información comercial confidencial, diseños de software y patentes.

Cumplimiento normativo/licencias de software: tiene que ver con software que no está actualizado o no cumple la normativa, o parches que no se instalan a tiempo.

Hay muchos recursos, como el NIST, que proporcionan listas de

riesgos de ciberseguridad

. Además, el Open Web Application Security Project (OWASP) publica un documento estándar de concientización sobre los

10 riesgos de seguridad más críticos

para las aplicaciones web, que se actualiza regularmente.

Nota: La lista de tipos de ataques frecuentes de OWASP contiene tres nuevos riesgos para los años 2017 a 2021: diseño inseguro, fallas de integridad del software y los datos, y falsificación de solicitudes del lado del servidor. Esta actualización enfatiza el hecho de que la seguridad es un campo en constante evolución. También demuestra la importancia de mantenerse al día sobre las tácticas y técnicas usadas por los agentes de amenaza, para que puedas prepararte mejor para manejar este tipo de riesgos.

Listas que comparan los 10 tipos de ataques más frecuentes entre 2017 y 2021

Vulnerabilidades

Una vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza. Por lo tanto, las organizaciones deben inspeccionar periódicamente sus sistemas en busca de vulnerabilidades. Algunas de estas pueden ser:

ProxyLogon: una vulnerabilidad preautenticada que afecta al servidor de Microsoft Exchange. Esto significa que un agente de amenaza puede completar un proceso de autenticación de usuario para implementar código malicioso desde una ubicación remota.

ZeroLogon: una vulnerabilidad en el protocolo de autenticación Netlogon de Microsoft. Un protocolo de autenticación es una forma de verificar la identidad de una persona. Netlogon es un servicio que garantiza la identidad de un usuario antes de permitirle el acceso a la ubicación de un sitio web.

Log4Shell: posibilita a los atacantes ejecutar código Java en la computadora de otra persona o filtrar información confidencial. Para ello, permite a un atacante remoto tomar el control de dispositivos conectados a Internet y ejecutar código malicioso.

PetitPotam: afecta al gestor de redes de área local (LAN) de nueva tecnología de Windows (NTLM). Se trata de una técnica de robo que permite a un atacante basado en LAN iniciar una solicitud de autenticación.

Fallos de registro y supervisión de la seguridad: capacidades de registro y supervisión insuficientes que dan lugar a que quienes perpetran un ataque aprovechen vulnerabilidades sin que la organización lo sepa.

Falsificación de solicitudes del lado del servidor: permite a quienes perpetran un ataque manipular una aplicación del lado del servidor para que acceda a recursos backend y los actualice. También puede permitir que los agentes de amenaza roben datos.

Como analista de seguridad de nivel inicial, podrías encargarte de la gestión de vulnerabilidades, que consiste en monitorear un sistema para identificarlas y mitigarlas. Aunque existan parches y actualizaciones, si no se aplican, pueden producirse intrusiones. Por esta razón, el seguimiento constante es clave. Cuanto más temprano identifique una organización una vulnerabilidad y la aborde aplicando parches o actualizando sus sistemas, antes se podrá mitigar, reduciendo su exposición a la vulnerabilidad.

Conclusiones clave

En esta lectura, aprendiste sobre algunas estrategias y marcos de gestión de riesgos que se pueden utilizar para desarrollar políticas y procesos en toda la organización con el objetivo de mitigar amenazas, riesgos y vulnerabilidades. También, obtuviste información sobre algunas de las amenazas, riesgos y vulnerabilidades más comunes en la actualidad para las operaciones comerciales. Comprender estos conceptos puede prepararte mejor no solo para proteger, sino también para mitigar los tipos de problemas relacionados con la seguridad que pueden dañar tanto a las organizaciones como a las personas.

Recursos para obtener más información

Para obtener más información, haz clic en los términos vinculados en esta lectura. Considera también la posibilidad de revisar los siguientes sitios:

OWASP Top Ten

NIST RMF

**Conclusión**

¡Acabas de completar la primera parte de este curso! Repasemos lo aprendido hasta ahora. Empezamos explorando el enfoque de los ocho dominios de seguridad del CISSP. Luego, vimos amenazas, riesgos y vulnerabilidades, y cómo pueden afectar a las organizaciones. Analizamos de cerca el ransomware y presentamos las tres capas de la web. Por último, vimos los siete pasos del Marco de Gestión de Riesgos del NIST, también llamado RMF. Felicidades por ampliar tus conocimientos en análisis de seguridad. En los próximos videos, profundizaremos en más detalles sobre algunas herramientas comunes utilizadas por analistas de seguridad de nivel inicial. Luego, tendrás la oportunidad de analizar los datos generados por esas herramientas para identificar riesgos, amenazas o vulnerabilidades. También tendrás la oportunidad de usar un manual de estrategias para responder a incidentes. Es todo por ahora. ¡Sigue así!

**Términos del glosario**

Amenaza externa: Cualquier cosa fuera de la organización que tenga el potencial de dañar los activos de esta.

Amenaza interna: Riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella.

Autorizar: Sexto paso del Marco de Gestión de Riesgos (RMF) del NIST, que se refiere a asumir la responsabilidad de los riesgos de seguridad y privacidad que puedan existir en una organización.

Categorizar: Segundo paso del Marco de Gestión de Riesgos (RMF) del NIST, que se lleva a cabo para desarrollar procesos y tareas de gestión de riesgos.

Continuidad del negocio: Capacidad de una organización para mantener su productividad diaria mediante el establecimiento de planes de recuperación de riesgos de desastre.

Evaluar: Quinto paso del Marco de Gestión de Riesgos (RMF) del NIST, para determinar si los controles establecidos se han implementado correctamente.

Implementar: Cuarto paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en aplicar planes de seguridad y privacidad en una organización.

Ingeniería social: Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

Monitorear: Séptimo paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en evaluar cómo están funcionando los sistemas.

Postura de seguridad: Capacidad de una organización para administrar la defensa de sus activos y datos críticos, y de reaccionar ante los cambios.

Preparar: Primer paso del Marco de Gestión de Riesgos (RMF) del NIST, relacionado con las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una vulneración.

Ransomware (secuestro de datos): Ataque malicioso en el que quien lo perpetra cifra los datos de una organización y exige un pago (rescate) para restablecer el acceso a ellos.

Reducción del riesgo: Proceso de disponer de los procedimientos y reglas adecuados para reducir rápidamente el impacto de un riesgo, como una vulneración.

Responsabilidad compartida: Idea de que todos los individuos dentro de una organización asumen un papel activo en la reducción del riesgo y el mantenimiento de la seguridad física y virtual.

Riesgo: Cualquier cosa que pueda afectar a la confidencialidad, integridad o disponibilidad de un activo.

Seleccionar: Tercer paso del Marco de Gestión de Riesgos (RMF) del NIST, que consiste en elegir, personalizar y capturar la documentación de los controles que protegen a una organización.

Vulnerabilidad: Debilidad que puede ser aprovechada por una amenaza.

¡Hola de nuevo! Como analista de ciberseguridad, tu trabajo no solo consiste en proteger a tu organización. Tu rol es mucho más importante. También ayudas a proteger a la gente. Las fallas de seguridad que afectan a los datos del personal, proveedores y clientes pueden dañar de forma significativa la estabilidad financiera y reputación de las personas. Como analista, tu trabajo cotidiano ayudará a proteger a las organizaciones y a la gente. En esta sección del curso, veremos los marcos, controles, y principios de diseño de seguridad con detalle, y cómo pueden aplicarse a las auditorías de seguridad para proteger a las organizaciones y a la gente. Proteger la información confidencial del cliente es clave en mi trabajo cotidiano en Google. El marco de ciberseguridad del NIST es muy importante en esto. El marco garantiza la protección y cumplimiento de herramientas del cliente y dispositivos de trabajo personales mediante controles. Te presento el mundo de los marcos y controles de seguridad. ¡Empecemos!

**Marcos**

En una organización, se establecen planes de protección contra varias de amenazas, riesgos y vulnerabilidades. Sin embargo, los requisitos utilizados para proteger a las personas y a las organizaciones suelen superponerse. Por esta razón, las organizaciones utilizan marcos de seguridad como punto de partida para crear sus políticas y procesos de seguridad. Repasemos qué son los marcos. Los marcos de seguridad son pautas usadas para crear planes para mitigar riesgos y amenazas contra los datos y la privacidad, como los ataques de ingeniería social y ransomware. La seguridad va más allá del espacio virtual. También incluye el espacio físico, por lo que muchas organizaciones tienen planes para proteger el entorno de laboral. Por ejemplo, el acceso a un edificio puede requerir el uso de una tarjeta o credencial. Otros marcos de seguridad indican cómo prevenir, detectar y responder a las fallas de seguridad. Esto es muy importante al proteger a una organización contra ataques de ingeniería social, como el phishing dirigido a empleados/as. Recuerda, las personas son la mayor amenaza para la seguridad. Los marcos pueden usarse para crear planes que aumenten la conciencia del personal y le enseñe sobre cómo puede proteger a la organización, a sus colegas y a sí mismo. Educar a los/las empleados/as sobre los desafíos de seguridad es esencial para minimizar la posibilidad de una filtración. Capacitar a los/las empleados/as para reconocer señales de alarma o amenazas potenciales es esencial, así como disponer de planes para reportar y abordar problemas rápidamente. Como analista, deberás comprender e implementar los planes que haya para proteger a la organización, sus empleados/as y usuarios/as contra ataques de ingeniería social, fallas y otros incidentes de seguridad. A continuación, veremos los controles seguridad, que se usan con los marcos para alcanzar los objetivos de seguridad de una organización.

**Controles**

Mientras que los marcos se utilizan para crear planes para abordar riesgos, amenazas y vulnerabilidades de seguridad, los controles sirven para reducir riesgos específicos. Si no se implementan los controles adecuados, una organización podría enfrentar impactos financieros significativos y daños a su reputación debido a la exposición a riesgos que incluyen intrusiones, creación de cuentas falsas de empleados/as o proporcionar beneficios gratuitos. Repasemos qué son los controles. Los controles de seguridad son medidas de protección diseñadas para reducir riesgos específicos. En este video, veremos tres tipos comunes de controles: cifrado, autenticación y autorización. El cifrado es el proceso de convertir datos de un formato legible a uno codificado. Suele implicar convertir datos de texto sin formato a texto cifrado. El texto cifrado es el mensaje codificado en bruto que es ilegible para humanos y computadoras. Los datos de texto cifrado no pueden leerse hasta descifrarlos y restaurar el texto sin formato. El cifrado se utiliza para la confidencialidad de datos sensibles, como la información de cuentas o números de seguridad social. Otro control que puede usarse para proteger datos sensibles es la autenticación. La autenticación se refiere a verificar la identidad de alguien o algo. Un ejemplo de autenticación real es iniciar sesión con nombre de usuario y contraseña. Esta autenticación básica demuestra que conoces el nombre de usuario y contraseña, y se te debe dar acceso. Los métodos más avanzados de autenticación, como la autenticación de múltiples factores (MFA), someten al usuario a demostrar que es quien dice ser requiriendo una contraseña y un formulario extra de autenticación, como un código de seguridad o datos biométricos, como una huella dactilar, voz o verificación facial. La biometría se refiere a características físicas únicas que pueden usarse para verificar identidades. Por ejemplo, una huella dactilar, un escaneo ocular o de la palma de la mano. El vishing es un ejemplo de ataque de ingeniería social que aprovecha los datos biométricos. El vishing es el aprovechamiento de la comunicación electrónica de voz para obtener información sensible para hacerse pasar por una fuente conocida. Por ejemplo, el vishing podría usarse para suplantar la voz de una persona y robar su identidad para cometer un delito. Otro control de seguridad muy importante es la autorización.

Reproduce el video desde :2:51 y sigue la transcripción2:51

La autorización es el concepto de conceder acceso a recursos específicos dentro de un sistema. Básicamente, la autorización se utiliza para verificar que una persona tiene permiso para acceder a un recurso.

Reproduce el video desde :3:6 y sigue la transcripción3:06

Por ejemplo, si trabajas como analista de seguridad de nivel inicial para el gobierno federal, podrías tener permiso para acceder a datos a través de la deep web o a otros datos internos solo accesibles si trabajas para el gobierno federal. Los controles de seguridad vistos son solo un elemento de una guía básica de seguridad conocida como la tríada CID. A continuación, veremos más de esta y cómo los equipos de seguridad la usan para proteger a las organizaciones.

Cómo se vinculan los marcos y los controles

Anteriormente, viste de qué modo las organizaciones usan marcos y controles de seguridad para protegerse contra amenazas, riesgos y vulnerabilidades. Esto incluye debates sobre el Marco de Gestión de Riesgos (RMF) y el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), así como la tríada de confidencialidad, integridad y disponibilidad (CID). En esta lección, aprenderás un poco más sobre los marcos y controles de seguridad cibernética y cómo se pueden combinar para mitigar los riesgos empresariales.

Marcos y controles

Los marcos de seguridad son pautas utilizadas para elaborar planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad. Estos marcos brindan soporte a las organizaciones para acatar las leyes y las normas de cumplimiento. Por ejemplo, en el sector de la salud se utilizan marcos para cumplir con la Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA) de los Estados Unidos, que exige a profesionales médicos mantener a resguardo la información de sus pacientes.

Los controles de seguridad, en tanto, son medidas de protección diseñadas para reducir riesgos de seguridad específicos. Estas medidas son utilizadas por las organizaciones para disminuir los riesgos y amenazas a los datos y la privacidad. Por ejemplo, una medida de control que se puede usar junto con los marcos de seguridad para garantizar que el cumplimiento de HIPAA en un hospital es requerir que las y los pacientes utilicen autenticación de múltiples factores (MFA) para acceder a sus registros médicos. El uso de una medida como la MFA para validar la identidad de las personas es una manera de ayudar a mitigar posibles riesgos y amenazas a la seguridad de los datos privados.

Marcos y controles específicos

Existen diversos marcos y controles que las organizaciones pueden utilizar para cumplir con las regulaciones y alcanzar sus objetivos de seguridad. Los marcos abordados en esta lección son el Marco de Amenaza Cibernética (Cyber Threat Framework, CTF) y la Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27001. También se explican varios controles de seguridad comunes, que se usan junto con este tipo de marcos.

Marco de Amenaza Cibernética (Cyber Threat Framework, CTF)

De acuerdo con la Oficina del Director de Inteligencia Nacional, el CTF fue desarrollado por el gobierno de los Estados Unidos con el fin de proporcionar “un lenguaje común para describir y comunicar información sobre la actividad de amenazas cibernéticas”. Al ofrecer un lenguaje común, el CTF ayuda a las y los profesionales de ciberseguridad a analizar y compartir información de manera más eficiente. Esto permite a las organizaciones mejorar su respuesta, dado que las tácticas y técnicas de los agentes de amenaza son múltiples y, por lo tanto, la ciberseguridad está en constante evolución.

Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27001

Un marco reconocido internacionalmente y muy utilizado es el ISO/IEC 27001. El conjunto de normas ISO 27000 permite a las organizaciones de todos los sectores y tamaños gestionar la seguridad de sus activos, como la información financiera, la propiedad intelectual, los datos del personal y la información confiada a terceros. Este marco establece los requisitos para un sistema de gestión de seguridad de la información, las prácticas recomendadas y los controles que respaldan la capacidad de una organización para gestionar los riesgos. Si bien el marco ISO/IEC 27001 no exige el uso de controles específicos, proporciona una serie de controles que las empresas pueden utilizar para mejorar su postura de seguridad.

Controles

Los controles se utilizan junto con los marcos para reducir la posibilidad y el impacto de una amenaza, riesgo o vulnerabilidad de seguridad. Estos pueden ser físicos, técnicos y administrativos, y se utilizan típicamente para prevenir, detectar o corregir problemas de seguridad.

Ejemplos de controles físicos:

Puertas, barreras y cerraduras

Guardias de seguridad

Vigilancia por circuito cerrado de televisión (CCTV), cámaras y detectores de movimiento

Tarjetas de acceso o credenciales para ingresar a los espacios de la oficina

Ejemplos de controles técnicos:

Cortafuegos (firewalls)

Autenticación de múltiples factores (MFA)

Software de antivirus

Ejemplos de controles administrativos:

Separación de funciones

Autorización

Clasificación de activos

Para obtener más información sobre los controles, especialmente aquellos utilizados para proteger activos relacionados con la salud de diversos tipos de amenazas, consulta la

presentación sobre Control de Acceso Físico

del Departamento de Salud y Servicios Humanos de los Estados Unidos.

Conclusiones clave

Los marcos y controles de ciberseguridad se utilizan conjuntamente para establecer la postura de seguridad de una organización. Además, respaldan la capacidad de una empresa para alcanzar sus objetivos de seguridad y cumplir con leyes y regulaciones. Si bien estos marcos y controles suelen ser de adhesión voluntaria, se recomienda a las organizaciones implementarlos y utilizarlos para garantizar la seguridad de los activos críticos.

**Explora la tríada CID**

¡Me alegro de verte de nuevo! Como analista de seguridad de nivel inicial, tu principal responsabilidad es ayudar a proteger los activos y datos sensibles de tu organización de agentes de amenaza. La tríada CID es un modelo de seguridad fundamental que te ayudará a lograrlo. En este video, veremos la tríada CID y hablaremos de la importancia de cada componente para prevenir amenazas, riesgos y vulnerabilidades. ¡Empecemos! La tríada CID es un modelo que ayuda a las organizaciones a evaluar los riesgo y configurar sistemas y políticas de seguridad. Recuerda que las tres letras de la tríada CID significan confidencialidad, integridad y disponibilidad. Como analista de nivel inicial, mencionarás con frecuencia estos tres principios básicos al proteger a la organización y sus usuarios/as. La confidencialidad implica que solo los usuarios autorizados tienen acceso a ciertos activos o datos. Los datos sensibles deben divulgarse solo a quien los necesita para que solo accedan a ellos quienes tengan autorización. La integridad implica que los datos sean correctos, auténticos y confiables. Determinar la integridad de los datos y analizar cómo se usan te ayudará, como profesional de seguridad, a decidir si estos son confiables o no. La disponibilidad implica que solo puedan acceder a los datos quienes tengan autorización. Los datos inaccesibles no son útiles y pueden impedir que las personas hagan su trabajo. Como profesional de seguridad, garantizar que los sistemas, redes y aplicaciones funcionen correctamente para dar acceso oportuno y confiable puede formar parte de tu trabajo cotidiano. Tras definir la tríada CID y sus componentes, veamos cómo podrías usarla para proteger a una organización. Si trabajas para una organización, como un banco, con muchos datos privados, el principio de confidencialidad es esencial porque el banco debe proteger la información financiera personal. El principio de integridad también es prioritario. Por ejemplo, si el gasto o las tiendas habituales de alguien cambian drásticamente, el banco probablemente deshabilitará el acceso a la cuenta hasta verificar que la compra la hace el propietario y no un agente de amenaza. El principio de disponibilidad también es crítico. Los bancos se esfuerzan para que la gente accedan fácilmente desde Internet a la información de su cuenta. Para proteger la información contra agentes de amenaza, se usa un proceso de validación que minimiza el daño si se sospecha que la cuenta del cliente está comprometida. Como analista, usarás con frecuencia cada componente de la tríada CID para proteger a la organización y sus usuarios/as. Tenerla constantemente en mente te ayudará a mantener la confidencialidad de datos y activos frente a amenazas, riesgos y vulnerabilidades, incluyendo ataques de ingeniería social, malware y el robo de datos que vimos anteriormente. A continuación, veremos marcos y principios específicos que también te ayudarán a prevenir amenazas, riesgos y vulnerabilidades. ¡Hasta pronto!

Usa la tríada CID para proteger a las organizaciones

Anteriormente, te presentamos la tríada de confidencialidad, integridad y disponibilidad (CID) y de qué modo ayuda a las organizaciones a evaluar y mitigar el riesgo. En esta lección, aprenderás cómo los/as analistas de ciberseguridad la utilizan en el entorno laboral.

Tríada CID para analistas

La tríada CID es una guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad. Está compuesta por tres elementos fundamentales: confidencialidad, integridad y disponibilidad. Las/los analistas de ciberseguridad trabajan en mantener estos elementos para asegurar un nivel de riesgo aceptable. Diseñar sistemas y políticas con estos elementos en mente ayuda a establecer una postura de seguridad exitosa. La postura de seguridad se refiere a la capacidad que tiene una organización para gestionar la defensa de sus activos y datos críticos, así como de reaccionar ante los cambios de manera efectiva.

Confidencialidad

La confidencialidad refiere a que solo los/las usuarios/as autorizados/as pueden acceder a activos o datos específicos. En una organización, la confidencialidad puede mejorarse mediante la implementación de principios de diseño, como el principio de mínimo privilegio, que limita el acceso de las personas solo a la información que necesitan para llevar a cabo las tareas laborales. Limitar el acceso es una forma de mantener la confidencialidad y la seguridad de los datos privados.

Integridad

La integridad implica que los datos son verificables, auténticos y confiables. Es esencial contar con protocolos para verificar la autenticidad de los datos y una manera de hacerlo es mediante la

criptografía

, que se utiliza para transformar los datos, para que las partes no autorizadas no puedan leerlos ni manipularlos (NIST, 2022). Otro ejemplo de cómo una organización podría implementar la integridad es mediante la activación del cifrado, que es el proceso de convertir los datos de un formato legible a uno codificado. Se puede utilizar para evitar el acceso a información, como los mensajes en la plataforma de chat interna de una organización.

Disponibilidad

La disponibilidad refiere a que los datos son accesibles para aquellas personas autorizadas a usarlos. Cuando un sistema cumple tanto los principios de disponibilidad como los de confidencialidad, los datos pueden ser utilizados cuando sea necesario. En el entorno laboral, esto puede significar que la organización permite al personal que trabaja de forma remota acceder a su red interna para desempeñar sus tareas laborales. Es importante tener en cuenta que el acceso a los datos en la red interna sigue siendo limitado, según el tipo de acceso que los/las empleados/as necesiten para realizar su trabajo. Si, por ejemplo, una persona trabaja en el departamento de Contabilidad de la empresa, es posible que necesite acceso a las cuentas corporativas, pero no a los datos relacionados con proyectos que estén desarrollando en ese momento.

Conclusiones clave

La tríada CID es esencial para determinar la postura de seguridad de una organización. Conocer qué es y cómo se aplica puede ayudarte a comprender mejor cómo los equipos de ciberseguridad trabajan para proteger a las empresas y a las personas.

**Marcos del NIST**

¡Hola de nuevo! Antes de empezar, repasemos rápidamente el propósito de los marcos. Las organizaciones los usan como punto de partida para crear planes que mitiguen riesgos, amenazas y vulnerabilidades contra datos y activos sensibles. Afortunadamente, hay organizaciones en todo el mundo que crean marcos que los/las profesionales de seguridad pueden usar para desarrollar esos planes. En este video, veremos dos marcos del Instituto Nacional de Estándares y Tecnología (NIST) que pueden apoyar el trabajo de seguridad de todo tipo de organizaciones, incluyendo empresas con y sin fines de lucro, así como agencias gubernamentales. Aunque el NIST es una organización de los EE.UU., sus pautas ayudan a analistas de todo el mundo a entender cómo implementar prácticas esenciales de ciberseguridad. Un marco del NIST que veremos en el programa es el marco de ciberseguridad (CSF) del NIST. El CSF es un marco voluntario que incluye estándares, pautas y mejores prácticas para manejar los riesgos de ciberseguridad. Este marco es muy respetado y esencial para mantener la seguridad, independientemente de dónde trabajes. El CSF consta de cinco funciones importantes. **Identificar, proteger, detectar, responder y recuperar**. Los veremos con detalle en un próximo video. Por ahora, nos centraremos en las ventajas del CSF y cómo se usan para prevenir amenazas, riesgos y vulnerabilidades con un ejemplo en el entorno laboral. Imagina que mañana recibes una notificación de alto riesgo de que un equipo se vio comprometido. Identificas el equipo, y descubres que hay un dispositivo desconocido conectado a él. Bloqueas el dispositivo de forma remota para detener cualquier potencial amenaza y proteger así a la organización. Luego retiras el equipo infectado para prevenir la propagación del daño y usas herramientas para detectar comportamientos del agente de amenaza e identificar el dispositivo desconocido. Respondes investigando el incidente para ver quién usó el dispositivo desconocido, cómo ocurrió la amenaza, qué se vio afectado y dónde se originó el ataque. En este caso, descubres que una empleada estaba cargando su teléfono infectado mediante un puerto USB en su computadora de trabajo. Por último, haces todo lo posible para recuperar los archivos o datos afectados y corregir cualquier daño que pudo haber ocasionado al equipo. Como lo demuestra el ejemplo anterior, las funciones básicas del CSF del NIST proporcionan pautas y orientaciones específicas a los profesionales de seguridad. Este marco se usa para desarrollar planes para manejar incidentes de forma correcta y rápida, reducir el riesgo, proteger contra una amenaza y mitigar posibles vulnerabilidades. El CSF del NIST también incluye la protección del gobierno federal de los EE.UU. con la publicación especial del NIST, SP 800-53. Ofrece un marco unificado para proteger los sistemas de información dentro del gobierno federal, incluyendo aquellos brindados por empresas privadas para uso federal. Los controles de seguridad de este marco se usan para mantener la tríada CID de esos sistemas usados por el gobierno. ¿No es increíble cómo estos marcos y controles funcionan de forma conjunta? Hemos discutido algunos temas de seguridad realmente importantes en este video que te serán muy útiles a medida que continúes tu recorrido en seguridad, pues son fundamentos de la profesión de seguridad.

El CSF del NIST es un marco útil que conocen la mayoría de los/las profesionales. Comprender la SP 800-53 del NIST es clave si te interesa trabajar para el gobierno federal de los EE.UU. A continuación, seguiremos explorando las cinco funciones del CSF del NIST y cómo las usan las organizaciones para proteger sus activos y datos.

**Explora las cinco funciones del Marco de Ciberseguridad (CSF) del NIST**

¡Hola de nuevo! Me emociona verte aquí. Tenemos mucho de qué hablar. Anteriormente, vimos los usos y ventajas del CSF del NIST. En este video, vamos a enfocarnos específicamente en las cinco funciones centrales del CSF del NIST. Comencemos. El CSF del NIST se enfoca en cinco funciones centrales: identificar, proteger, detectar, responder y recuperar.

Estas funciones ayudan a gestionar los riesgos de ciberseguridad, implementar estrategias de gestión y aprender de errores anteriores. Básicamente, en lo que respecta a las operaciones de seguridad, las funciones del CSF del NIST son clave para proteger a una organización contra amenazas, riesgos y vulnerabilidades potenciales. Tomemos un tiempo para explorar cómo cada función puede utilizarse para mejorar la seguridad.

La primera función central es **identificar**, que está relacionada con la gestión del riesgo de ciberseguridad y su efecto en las personas y activos de una organización. Por ejemplo, como analista de seguridad, es posible que se te solicite monitorear los sistemas y dispositivos en la red interna de la organización para identificar posibles problemas de seguridad, como dispositivos comprometidos en la red. La segunda función central es **proteger**. Es la estrategia utilizada para proteger a una organización mediante la implementación de políticas, procedimientos, capacitaciones y herramientas que ayudan a mitigar las amenazas de ciberseguridad. Por ejemplo, como analista de seguridad, tú y tu equipo podrían enfrentrar amenazas y ataques nuevos y desconocidos. Por esta razón, estudiar datos históricos y mejorar las políticas y procedimientos es esencial. La tercera función central es **detectar**. Es identificar posibles incidentes de seguridad y mejorar las capacidades de monitoreo para aumentar la velocidad y eficiencia de las detecciones. Por ejemplo, como analista, te pueden pedir que revises la configuración de una herramienta nueva para verificar que identifique riesgos bajos, medios o altos, y luego alertar al equipo de seguridad sobre cualquier amenaza o incidente potencial. La cuarta función es **responder**. Es tomar las medidas adecuadas para contener, neutralizar y analizar los incidentes de seguridad, e implementar mejoras en el proceso de seguridad. Como analista, podrías estar trabando con un equipo para recopilar y organizar datos a fin de documentar un incidente y sugerir mejoras en los procesos para evitar que se repita.

La quinta función es **recuperar**. Es restaurar la operación normal de los sistemas afectados.

Por ejemplo, como analista de seguridad de nivel inicial, podrías trabajar con tu equipo para restaurar los sistemas, datos y activos, como archivos financieros o legales afectados por un incidente como una falla de seguridad. Vimos mucha información en este video. Espero que te ayude a entender el valor de conocer sobre el CSF del NIST y sus cinco funciones. Con medidas proactivas y reactivas, las cinco funciones son esenciales para que una organización cuente con estrategias de seguridad efectivas. Habrá incidentes de seguridad, pero la organización debe poder recuperarse rápido de cualquier daño causado por un incidente para minimizar su nivel de riesgo. A continuación, veremos principios de seguridad que van mano a mano con los marcos del NIST y la tríada CID para ayudar a proteger los datos y activos críticos.

**Principios de seguridad de OWASP**

Es importante comprender cómo proteger los datos y activos de una organización porque esto formará parte de tu rol como analista de seguridad. Afortunadamente, hay principios y pautas que puedes usar, así como los marcos del NIST y la tríada CID para ayudar a los equipos a minimizar amenazas y riesgos. Aquí veremos algunos principios de seguridad del Open Web Application Security Project (OWASP) que son útiles para analistas de nivel inicial. **El primer principio de OWASP es minimizar el área de superficie de ataque**. Una superficie de ataque se refiere a toda vulnerabilidad potencial que un agente de amenaza podría aprovechar, como vectores de ataque, que son vías de acceso que los atacantes utilizan para penetrar las defensas de seguridad. Algunos ejemplos de vectores de ataque comunes son los correos de phishing y contraseñas poco seguras. Para minimizar la superficie de ataque y evitar incidentes de este tipo de vectores, los equipos pueden desactivar funciones del software, restringir quién puede acceder a ciertos activos o establecer requisitos de contraseña más complejos.

**El principio del privilegio mínimo** significa que los usuarios tengan el menor nivel de acceso necesario para realizar sus tareas diarias. La razón principal para limitar el acceso a la información y los recursos de la organización es reducir el daño que podría causar una violación de seguridad. Por ejemplo, como analista de nivel inicial, puede que tengas acceso a los datos de registro pero es posible que no tengas acceso para cambiar los permisos de usuario. Por lo tanto, si un agente de amenaza compromete tus credenciales, solo podrá obtener acceso limitado a los activos digitales o físicos, lo cual puede no ser suficiente para ejecutar su ataque. **El siguiente principio es la defensa en profundidad**. La defensa en profundidad significa que una organización debe tener varios controles de seguridad que aborden los riesgos y amenazas de distintas maneras. Un ejemplo de control de seguridad es la autenticación de múltiples factores (MFA), que requiere tomar un paso más allá de solo ingresar el nombre de usuario y contraseña para acceder a una aplicación. Otros controles son firewalls, sistemas de detección de intrusiones y configuraciones de permisos que pueden usarse para crear varios puntos de defensa que un agente de amenaza debe pasar para comprometer a una organización. Otro **principio es la separación de funciones**, que puede usarse para evitar que la gente lleve a cabo actividades fraudulentas o ilegales. Este principio dicta que nadie debe recibir tantos privilegios que pueda abusar del sistema. Por ejemplo, el/la empleado/a que firma las nóminas no debería ser también quien las prepara. Solo quedan dos principios más. ¡Lo estás haciendo genial! El siguiente **principio es simplificar la seguridad**. Tal como indica su nombre, al implementar controles de seguridad, deben evitarse soluciones innecesariamente complejas porque pueden ser difíciles de gestionar. Cuanto más complejos sean los controles de seguridad, más difícil es trabajar en colaboración.

El **último principio es corregir correctamente los problemas de seguridad**. La tecnología es una gran herramienta, pero también puede presentar desafíos. Cuando ocurre un incidente de seguridad, se espera que los/las profesionales de seguridad identifiquen la causa principal rápidamente. Luego es importante corregir cualquier vulnerabilidad identificada y efectuar pruebas para asegurar que las reparaciones sean exitosas.

Un ejemplo de un problema es una contraseña débil para acceder a la red Wi-Fi de la organización porque podría causar una falla de seguridad. Para solucionar este tipo de problemas, se podrían implementar políticas de contraseñas más estrictas. Sé que hemos cubierto mucho, pero comprender estos principios aumenta tu conocimiento general de seguridad y te ayudará a destacarte como profesional en este campo.

Más información sobre los principios de seguridad de OWASP

Anteriormente, aprendiste que las/los analistas de ciberseguridad ayudan a mantener los datos seguros y reducir el riesgo en una organización, mediante una variedad de marcos, controles y principios de seguridad. En esta lección, conocerás más sobre los principios de seguridad de Open Web Application Security Project (OWASP, por sus siglas en inglés) y cómo las/los analistas de nivel inicial los utilizan.

Principios de seguridad

En el entorno laboral, los principios de seguridad están integrados en las tareas diarias. Ya sea que estés analizando registros, monitoreando un panel de gestión de eventos e información de seguridad (SIEM) o usando un

escáner de vulnerabilidades

, utilizarás estos principios de alguna manera.

Anteriormente, te presentamos varios principios de seguridad de OWASP, que incluían:

Minimizar la superficie expuesta a ataques: se refiere a todas las vulnerabilidades potenciales que podría aprovechar un agente de amenaza.

Principio de mínimo privilegio: significa conceder únicamente el acceso y la autorización mínimos necesarios para completar una tarea o función.

Defensa en profundidad: hace referencia a que las organizaciones deben disponer de varios controles de seguridad que aborden los riesgos y las amenazas de diferentes maneras.

Separación de funciones: refiere a que las acciones críticas deben depender de varias personas, cada una de las cuales sigue el principio del mínimo privilegio.

Simplificar la seguridad: tiene que ver con evitar soluciones innecesariamente complicadas, porque la complejidad dificulta la seguridad.

Solucionar los problemas de seguridad correctamente: significa que, cuando ocurren incidentes de seguridad, es necesario identificar la causa, contener el impacto, detectar las vulnerabilidades y realizar pruebas para garantizar que la reparación sea exitosa.

Otros principios de seguridad de OWASP

A continuación, aprenderás acerca de otros cuatro principios de seguridad de OWASP que se utilizan para mantener seguras las operaciones de una organización y a las personas.

Establecer configuraciones seguras por defecto

Este principio indica que el estado de seguridad óptimo de una aplicación también debe ser su estado predeterminado para los/las usuarios/as. O sea, debería requerirse un esfuerzo adicional para hacer que la aplicación sea insegura.

Fallar de forma segura

Fallar de forma segura significa que, cuando un control falla o se detiene, debe hacerlo restableciéndose automáticamente a su opción más segura. Por ejemplo, si un cortafuegos (firewall) falla, simplemente, debería cerrar todas las conexiones y bloquear las nuevas, en lugar de comenzar a aceptar todo.

No confiar en los servicios

Muchas organizaciones trabajan con firmas asociadas o proveedoras de servicios. Estas suelen tener políticas de seguridad diferentes a las de la empresa. Por lo tanto, la compañía no debería dar por sentado que los sistemas de estas firmas sean seguros. Por ejemplo, si una aerolínea terceriza a una empresa proveedora el seguimiento de los puntos de recompensa, antes de compartir esa información con sus clientes, debería asegurarse de que los datos obtenidos y el saldo sean precisos.

Evitar la seguridad por oscuridad

La seguridad de los sistemas clave no debe depender de mantener los detalles ocultos. Analiza el siguiente ejemplo de OWASP (2016):

La seguridad de una aplicación no debe depender de mantener el código fuente en secreto, sino que su seguridad tiene que basarse en muchos otros factores, como las políticas de contraseñas razonables, la defensa en profundidad, los límites de transacciones comerciales, una sólida arquitectura de red, y los controles de fraude y auditoría.

Conclusiones clave

Las y los profesionales de la ciberseguridad aplican constantemente los principios de seguridad para proteger a las organizaciones y a las personas. Como analista de ciberseguridad de nivel inicial, puedes utilizar estos principios para implementar prácticas seguras que reduzcan los riesgos tanto para las empresas como para los/las usuarios/as.

**Mantente al día de las amenazas de ciberseguridad más recientes**

**Planifica una auditoría de seguridad**

Tras ver diversos marcos, controles, principios de seguridad y cumplimiento normativo, la pregunta es: ¿Cómo funciona todo junto? La respuesta es: mediante auditorías de seguridad. Esta es una revisión de los controles de seguridad, políticas y procedimientos que tiene una organización. Existen dos tipos principales de auditorías de seguridad: externas e internas. Nos centraremos en las internas porque ese es el tipo de auditorías al que contribuyen los/las analistas de nivel inicial. La auditoría interna de seguridad la suele realizar un equipo de personas que puede incluir al encargado/a de cumplimiento, gerente de seguridad y otros miembros del equipo. Las auditorías internas de seguridad se utilizan para mejorar la postura de seguridad de una organización y evitar multas de agencias reguladoras por falta de cumplimiento normativo. Con la auditoría interna, el equipo identifica el riesgo organizacional, evalúa los controles y corrige problemas de cumplimiento. Ahora, que hemos discutido los propósitos de las auditorías internas, veamos algunos de sus componentes comunes. Estos son definir el alcance y los objetivos de la auditoría, evaluar el riesgo de los activos de la organización, evaluar los controles, evaluar el cumplimiento y comunicar los resultados a las partes interesadas. En este video, veremos los primeros dos elementos, que conforman el proceso de planificación: definir el alcance y los objetivos, y evaluar el riesgo. El alcance se refiere a los criterios de una auditoría interna. El alcance requiere identificar las personas, activos, políticas, procedimientos y tecnologías que podrían afectar a la postura de seguridad. Los objetivos son un planteo de las metas de seguridad o qué se quiere lograr para mejorar la postura de seguridad. Aunque los miembros de mayor jerarquía del equipo de seguridad y otras partes interesadas suelen definir el alcance y los objetivos, a los/las analistas de nivel inicial se les puede pedir que revisen el alcance y los objetivos para completar otros elementos de la auditoría. A modo de ejemplo, el alcance de esta auditoría implica evaluar los permisos del usuario, identificar los controles, políticas y procedimientos actuales y tener en cuenta la tecnología utilizada actualmente por la organización. Los objetivos señalados incluyen implementar funciones centrales de los marcos, como el CSF del NIST, definir políticas y procedimientos para garantizar el cumplimiento normativo, y fortalecer los controles del sistema. El siguiente elemento es evaluar el riesgo, que se centra en identificar amenazas, riesgos, y vulnerabilidades potenciales. Esto ayuda a las organizaciones a decidir qué medidas de seguridad implementar y monitorear para proteger sus activos. Al igual que definir el alcance y los objetivos, suelen evaluar el riesgo los/las gerentes u otras partes interesadas. Pero se te puede pedir que analices los detalles de la evaluación del riesgo para ver qué tipos de controles y normativa de cumplimiento se necesita tener para mejorar la postura de seguridad organizacional. Por ejemplo, esta evaluación del riesgo destaca que hay controles, procesos y procedimientos inadecuados para proteger los activos. En particular, falta un manejo adecuado de activos físicos y digitales, incluidos los equipos del personal. El equipo usado para almacenar datos no está bien protegido. Y el acceso a información privada almacenada en la red interna necesita tener controles más sólidos. Tras ver los elementos iniciales de la planificación de una auditoría de seguridad interna, veremos los tres últimos elementos.

Antes vimos los elementos iniciales de una auditoría interna de seguridad. En este video, veremos los elementos finales que un/a analista de nivel inicial podría tener que completar. Recuerda: los elementos de planificación de las auditorías internas son definir el alcance y los objetivos, y evaluar los riesgos.

Reproduce el video desde ::25 y sigue la transcripción0:25

Los elementos restantes son evaluar los controles, evaluar el cumplimiento y comunicar los resultados. Antes de completar los tres elementos finales debes consultar el alcance y los objetivos, así como la evaluación del riesgo, y plantearte algunas preguntas. Por ejemplo: ¿Qué se quiere lograr con la auditoría? ¿Qué activos están más en riesgo? ¿Son suficientes los controles actuales para proteger esos activos? Si no lo son, ¿qué controles y normativa de cumplimiento se deben implementar? Al tener en cuenta estas preguntas dispondrás de una base para completar el siguiente elemento: evaluar los controles.

Reproduce el video desde :1:10 y sigue la transcripción1:10

Una evaluación de controles implica revisar los activos de una organización y luego evaluar los posibles riesgos para esos activos a fin de garantizar que los controles internos sean efectivos. Para lograrlo, los/las analistas de nivel inicial podrían clasificar los controles en las siguientes categorías. Controles administrativos, controles técnicos y controles físicos. Los controles administrativos se relacionan con el componente humano de la ciberseguridad. Son políticas y procedimientos que definen cómo una organización gestiona los datos, como la implementación de las políticas de contraseñas. Los controles técnicos son soluciones de hardware y software para proteger los activos, como usar sistemas de detección de intrusiones (IDS) y cifrado.

Reproduce el video desde :2:7 y sigue la transcripción2:07

Los controles físicos son medidas implementadas para evitar el acceso físico a los activos protegidos, como cámaras de vigilancia y cerraduras. El siguiente elemento es determinar si la organización sigue o no el cumplimiento normativo necesaria. Recuerda, el cumplimiento normativo se refiere a leyes que la organización debe seguir para proteger los datos privados. En este ejemplo, la organización opera en la Unión Europea y acepta pagos con tarjeta de crédito. Por lo tanto, debe cumplir con el RGPD y los estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS). El elemento final de una auditoría interna de seguridad es la comunicación. Tras completar la auditoría interna, deben notificarse los resultados y recomendaciones a las partes interesadas. En general, este tipo de comunicación resume el alcance y los objetivos de la auditoría. Enumera los riesgos existentes e indica con qué velocidad deben abordarse. Además, identifica el cumplimiento normativo que la organización debe seguir y da recomendaciones para mejorar la postura de seguridad de la empresa. Las auditorías internas sirven para identificar vulnerabilidades dentro de la organización. En mi empleo anterior, llevé adelante junto con mi equipo una auditoría interna de contraseñas y descubrimos que muchas eran poco seguras. Tras identificar este problema, el equipo de cumplimiento tomó la iniciativa e implementó políticas de contraseña más estrictas. Las auditorías permiten determinar qué medidas de seguridad hay y qué áreas deben mejorarse para lograr la postura de seguridad deseada. Las auditorías de seguridad son complejas, pero aportan mucho valor a la organización. Más adelante, podrás completar elementos de una auditoría interna de seguridad de una empresa ficticia, la cual podrás incluir en tu cartera profesional.

¡Buen trabajo! Pudiste aprender más sobre los conceptos de seguridad que pueden ayudar a una organización a proteger sus datos y activos. Hemos visto bastante, pero todo ese conocimient será valioso para ti a medida que continúes hacia la profesión de la ciberseguridad. Primero definimos qué son los marcos de seguridad y cómo ayudan a las organizaciones a proteger la información crítica. También exploramos los controles de seguridad y su importancia en la protección contra riesgos, amenazas y vulnerabilidades. Hablamos de la tríada CID, que es un modelo de seguridad central, y dos marcos del NIST: el CSF y el SP 800-53. Luego vimos algunos principios de diseño seguro del OWASP. Terminamos presentando las auditorías de seguridad con un enfoque en los elementos de una auditoría interna que te pueden pedir completar o contribuir en ella. Los/las profesionales de seguridad usan los conceptos que discutimos para proteger los activos de las organizaciones, sus datos, sistemas y personas. A medida que continúes en tu camino hacia la profesión de ciberseguridad, aparecerán de manera repetida muchos de estos conceptos. Ahora te estamos brindando una comprensión fundamental de las prácticas y temas de seguridad que te serán de utilidad. En la siguiente sección, veremos herramientas de seguridad que podrías usar un día como analista. Abordaremos cómo utilizarlas para mejorar la postura de seguridad de una organización y cómo pueden ayudarte a proteger a las organizaciones y a las personas. Me entusiasma continuar contigo. ¡Hasta pronto!

Términos y definiciones del curso 2, semana 2

Activo: Elemento percibido como valioso para una organización.

Amenaza: Cualquier circunstancia o evento que pueda afectar los activos de manera negativa.

Auditoría de seguridad: Revisión de los controles, políticas y procedimientos de seguridad de una organización.

Autenticación: Proceso de verificar la identidad de una persona.

Autorizar: Sexto paso del Marco de Gestión de Riesgos (RMF) del NIST que se refiere a asumir la responsabilidad de los riesgos de seguridad y privacidad que puedan existir en una organización.

Cifrado: El proceso de convertir datos de un formato legible a uno legible con el fin de protegerlos.

Confidencialidad: Propiedad según la cual únicamente las personas autorizadas pueden acceder a activos o datos específicos.

Controles de seguridad: Medidas de prevención diseñadas para reducir riesgos de ciberseguridad específicos.

Datos biométricos: Características físicas únicas que se pueden utilizar para verificar la identidad de una persona.

Detectar: Una función central del NIST relacionada con la identificación de posibles incidentes de seguridad y la mejora de las capacidades de monitoreo y respuesta.

Disponibilidad: Propiedad según la cual todas las personas autorizadas pueden acceder a activos o datos específicos.

Identificar: Una función central del NIST relacionada con la gestión del riesgo de ciberseguridad y su efecto sobre las personas y los activos de una organización.

Integridad: Cualidad que identifica a los datos como correctos, auténticos y confiables.

Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST): Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar los riesgos de ciberseguridad.

Marcos de seguridad: Pautas utilizadas para crear planes que ayuden a mitigar el riesgo y las amenazas a los datos y la privacidad.

Open Web Application Security Project (OWASP): Organización sin fines de lucro centrada en mejorar la seguridad del software.

Postura de seguridad: Capacidad de una organización para administrar la defensa de sus activos y datos críticos y reaccionar ante los cambios.

Proteger: Una función central del NIST que consiste en resguardar a una organización a través de la implementación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas a la ciberseguridad.

Publicación Especial (SP) del Instituto Nacional de Normas y Tecnología (NIST) 800-53: Marco unificado para proteger la seguridad de los sistemas de información dentro del gobierno federal de los EE.UU.

Responder: Funciónunción central del NIST que consiste en restablecer el funcionamiento normal de los sistemas afectados.

Respuesta: Una función central del NIST relacionada con asegurarse de que se utilicen los procedimientos adecuados para contener, neutralizar y analizar incidentes de seguridad, e implementar mejoras en el proceso de seguridad.

Riesgo: Cualquier hecho que pueda afectar a la confidencialidad, integridad o disponibilidad de un activo.

Tríada de confidencialidad, integridad y disponibilidad (CID): Guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad.

Vector de ataque: Método que se utiliza para penetrar las defensas de seguridad de un sistema informático.