**Dominios de Seguridad CISSP**

**Postura de seguridad**

La postura de seguridad se refiere a la capacidad de una organización para gestionar su defensa de los activos y datos críticos y reaccionar ante los cambios.

**Dominios:**

**I. la gestión de seguridad y riesgos.**

Hay varias áreas de interés para este dominio: definición de metas y objetivos de seguridad, mitigación de riesgos, cumplimiento, continuidad del negocio y regulaciones legales.

Al **definir las metas y objetivos de seguridad**, las organizaciones pueden reducir los riesgos para los recursos y datos críticos como la PII, o información de identificación personal. **Mitigar los riesgos** significa disponer de los procedimientos y normas adecuados para reducir rápidamente el impacto de un riesgo como una violación. El C**umplimiento normativo** es el método principal utilizado para desarrollar las políticas de seguridad internas de una organización, los requisitos reglamentarios y las normas independientes. La **Continuidad del negocio** se refiere a la capacidad de una organización para mantener su productividad diaria mediante el establecimiento de planes de recuperación ante desastres por riesgos. Y por último, aunque las **leyes** relacionadas con la seguridad y la gestión de riesgos son diferentes en todo el mundo, los objetivos generales son similares.

**II. La seguridad de los activos**

El dominio de la seguridad de los activos se centra en proteger los activos digitales y físicos. También está relacionado con el almacenamiento, mantenimiento, retención y destrucción de datos. Esto significa que los recursos como la PII o la SPII deben manejarse de forma segura y protegerse, tanto si se almacenan en una computadora, se transfieren a través de una red como Internet o incluso se recogen físicamente.

Las organizaciones también necesitan contar con políticas y procedimientos que garanticen que los datos se almacenan, mantienen, conservan y destruyen correctamente. Saber qué datos se tienen y quién tiene acceso a ellos es necesario para tener una postura de seguridad sólida que mitigue el riesgo para los recursos y datos críticos. Por ejemplo, una organización puede pedirle, como analista de seguridad, que supervise la destrucción de discos duros para asegurarse de que se eliminan adecuadamente. Esto garantiza que los datos privados almacenados en esos discos no puedan ser accedidos por agentes de amenazas.

**III. La arquitectura de seguridad y la ingeniería**

Este dominio se centra en optimizar la seguridad de los datos garantizando que existen herramientas, sistemas y procesos eficaces para proteger los recursos y los datos de una organización. Uno de los conceptos centrales de la arquitectura de diseño seguro es la Responsabilidad compartida. Responsabilidad compartida significa que todas las personas de una organización asumen un papel activo en la reducción del Riesgo y en el mantenimiento de la Seguridad tanto física como virtual. Contar con políticas que animen a los usuarios a reconocer y notificar los problemas de seguridad permite gestionar muchos problemas de forma rápida y eficaz.

**IV. La seguridad de las comunicaciones y las redes**

Se centra en gestionar y proteger las redes físicas y las comunicaciones inalámbricas. Las redes seguras mantienen a salvo los datos y las comunicaciones de una organización ya sea in situ, en la nube o cuando se conecta a servicios de forma remota.

Por ejemplo, los empleados que trabajan a distancia en espacios públicos necesitan estar protegidos frente a las vulnerabilidades que pueden producirse cuando utilizan conexiones bluetooth inseguras o puntos de acceso wifi públicos. Al hacer que los miembros del Equipo de Seguridad eliminen el acceso a esos tipos de canales de comunicación a nivel organizativo, se puede disuadir a los empleados de practicar comportamientos inseguros que podrían ser explotados por agentes de amenaza.

**V. La Gestión de identidad y acceso, o IAM.**

Se centra en el acceso y la autorización para mantener los datos seguros asegurándose de que los usuarios siguen las políticas establecidas para controlar y gestionar los activos. Como analista de nivel básico, es esencial mantener los sistemas y datos de una organización tan seguros como sea posible asegurándose de que el acceso de los usuarios se limita a lo que los empleados necesitan. Básicamente, el objetivo de la IAM es reducir el riesgo global para los sistemas y los datos.

Por ejemplo, si todo el mundo en una empresa utiliza el mismo inicio de sesión de administrador, no hay forma de rastrear quién tiene acceso a qué datos. En caso de infracción, separar la actividad de un usuario válido del agente de amenaza sería imposible.

Hay cuatro componentes principales en la IAM. La **identificación** es cuando un usuario verifica quién es proporcionando un nombre de usuario, una tarjeta de acceso o datos biométricos como una huella dactilar. La **autenticación** es el proceso de verificación para probar la identidad de una persona, como introducir una contraseña o un PIN. La **autorización** tiene lugar una vez que se ha confirmado la identidad de un usuario y se relaciona con su nivel de acceso, que depende de la función que desempeñe en la organización. La **responsabilidad** se refiere a la supervisión y el registro de las acciones de los usuarios, como los intentos de inicio de sesión, para demostrar que los sistemas y los datos se utilizan correctamente.

**VI. La evaluación y las pruebas de seguridad**

Se centra en la realización de pruebas de control de la seguridad, la recopilación y el análisis de datos y la realización de auditorías de seguridad para supervisar los riesgos, las amenazas y las vulnerabilidades. Las pruebas de controles de seguridad pueden ayudar a una organización a identificar nuevas y mejores formas de mitigar las amenazas, los riesgos y las vulnerabilidades. Esto implica examinar las metas y objetivos de la organización y evaluar si los controles que se están utilizando realmente logran esas metas. Recopilar y analizar datos de seguridad regularmente también ayuda a prevenir amenazas y riesgos para la organización. Los analistas pueden utilizar las evaluaciones de las pruebas de controles de seguridad y los informes de evaluación de la seguridad para mejorar los controles existentes o implementar nuevos controles. Un ejemplo de implementación de un nuevo control podría ser exigir el uso de la autenticación de múltiples factores para proteger mejor a la organización de amenazas y riesgos potenciales.

**VII. Las operaciones de seguridad**

El ámbito de las operaciones de seguridad se centra en realizar investigaciones e implementar medidas preventivas. Las investigaciones comienzan una vez que se ha identificado un incidente de seguridad. Este proceso requiere un mayor sentido de la urgencia para minimizar los riesgos potenciales para la organización. Si hay un ataque activo, mitigar el ataque y evitar que siga escalando es esencial para garantizar que la información privada está protegida de los agentes de amenaza.

**VIII. La seguridad en el desarrollo de software**

Este dominio se centra en el uso de prácticas de programación seguras. Como recordará, las prácticas de codificación segura son directrices recomendadas que se utilizan para crear aplicaciones y servicios seguros. El ciclo de vida de desarrollo de software es un proceso eficiente utilizado por los equipos para crear rápidamente productos y funciones de software. En este proceso, la seguridad es un paso adicional. Al garantizar que cada fase del ciclo de vida de desarrollo de software se somete a revisiones de seguridad, la seguridad puede integrarse completamente en el producto de software.

Por ejemplo, realizar una revisión del diseño seguro durante la fase de diseño, revisiones del código seguro durante las fases de desarrollo y pruebas, y pruebas de penetración durante la fase de despliegue e implementación garantiza que la seguridad está integrada en el producto de software en cada paso. Esto mantiene el software seguro y los datos sensibles protegidos, y mitiga riesgos innecesarios para una organización.