**Marcos Y Controles De Seguridad**

**Los Marcos De Seguridad**

Los marcos de seguridad son directrices que se utilizan para crear planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad. Marcos de seguridad proporcionan un enfoque estructurado para implementar un ciclo de vida de seguridad. El ciclo de vida de la seguridad es un conjunto de políticas y normas en constante evolución que definen la forma en que una organización gestiona los riesgos, sigue las directrices establecidas y cumple con las leyes o el cumplimiento de las normativas.

Hay varios marcos de Seguridad que se pueden usar para administrar diferentes tipos de riesgos de cumplimiento normativo y organizacional. El propósito de los marcos de seguridad incluye proteger la información de identificación personal, conocida como PII, asegurar la información financiera, identificar las debilidades de seguridad, administrar los riesgos organizacionales y alinear la seguridad con los objetivos comerciales.

Los marcos tienen **cuatro** **componentes** principales y comprenderlos le permitirá gestionar mejor los riesgos potenciales.

El primer componente principal es **identificar** **y** **documentar** **los** **objetivos** **de** **Seguridad**. Por ejemplo, una organización puede tener el objetivo de alinearse con la UE».s Reglamento General de Protección de Datos, también conocido como GDPR. El RGPD es una ley de protección de datos establecida para conceder a los ciudadanos europeos un mayor control sobre sus datos personales. Es posible que se le pida a un analista de seguridad que identifique y documente las áreas en las que una organización no cumple con el GDPR.

El segundo componente principal es **establecer directrices para lograr los objetivos de Seguridad**. Por ejemplo, al implementar directrices para cumplir con el RGPD, es posible que su organización necesite desarrollar nuevas políticas sobre cómo gestionar las solicitudes de datos de los usuarios individuales.

El tercer componente central de los marcos de seguridad es **la implementación de procesos de seguridad sólidos**. En el caso del RGPD, un analista de Seguridad que trabaje para una empresa de redes sociales puede ayudar a diseñar procedimientos para garantizar que la organización cumpla con las solicitudes de datos de usuario verificadas. Un ejemplo de este tipo de solicitud es cuando un usuario intenta actualizar o eliminar la información de su perfil.

El último componente central de los marcos de Seguridad es **el monitoreo y la comunicación de los resultados**. Por ejemplo, puedes supervisar la red interna de tu organización e informar a tu gerente u oficial de cumplimiento normativo sobre un posible problema de Seguridad que afecte al RGPD.

Los marcos permiten a los analistas trabajar junto con otros miembros del equipo de Seguridad para documentar, implementar y usar las políticas y los procedimientos que se han creado. Es fundamental que un analista principiante comprenda este proceso, ya que afecta directamente al trabajo que realizan y a la forma en que colaboran con los demás. A continuación, analizaremos los controles de Seguridad.

**Controles de Seguridad**

Los **Controles** **de** **seguridad** son medidas de seguridad diseñadas para reducir los riesgos de seguridad específicos. Por ejemplo, es posible que su empresa tenga una directriz que obligue a todos los empleados a completar una formación sobre privacidad para reducir el riesgo de violaciones de datos. Como analista de Seguridad, puede utilizar una herramienta de software para asignar automáticamente y hacer un seguimiento de los empleados que han completado esta formación.

Los Marcos de seguridad y los controles son vitales para administrar la seguridad de todos los tipos de organizaciones y garantizar que todos hagan su parte para mantener un nivel de riesgo bajo.

La tríada CID de la CIA es un modelo fundamental que ayuda a informar cómo las organizaciones consideran el riesgo al establecer sistemas y políticas de Seguridad. CID es sinónimo de confidencialidad , integridad y disponibilidad.

La confidencialidad significa que solo los usuarios autorizados pueden acceder a activos o datos específicos. Por ejemplo, se deben establecer controles de acceso estrictos que definan quién debe y quién no debe tener acceso a los datos para garantizar que los datos confidenciales permanezcan seguros.

La integridad significa que los datos son correctos, auténticos y confiables. Para mantener la integridad, los profesionales de Seguridad pueden usar una forma de protección de datos, como la encriptación, para evitar que los datos sean manipulados.

Disponibilidad significa que los datos son accesibles para quienes están autorizados a acceder a ellos. Definamos un término que surgió durante nuestra discusión sobre la tríada CID de la CIA:

**recurso**.

Un recurso es un elemento que se percibe como valioso para una organización. Y el valor está determinado por el costo asociado con el recurso en cuestión. Por ejemplo, una aplicación que almacena datos confidenciales, como números de Seguridad Social o cuentas bancarias, es un recurso valioso para una organización. Conlleva más riesgos y, por lo tanto, requiere controles de Seguridad más estrictos en comparación con un sitio web que comparte contenido de noticias disponible públicamente.

Analizaremos un marco específico desarrollado por el Instituto Nacional de Estándares y Tecnología, con sede en EE. UU.: el Marco de Ciberseguridad, también conocido como NIST CSF. El marco de ciberseguridad del NIST es un marco voluntario que consiste en estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad.

Es importante familiarizarse con este framework porque los equipos de Seguridad lo utilizan como base para gestionar los riesgos a corto y largo plazo. Gestionar y mitigar los riesgos y proteger los activos de una organización contra los actores de amenazas son objetivos clave para los profesionales de la Seguridad. Es importante comprender los diferentes motivos que puede tener un actor de amenazas, además de identificar los activos más valiosos de su organización. Algunos de los actores de amenazas más peligrosos para tener en cuenta son los empleados descontentos. Son los más peligrosos porque a menudo tienen acceso a información confidencial y saben dónde encontrarla. Para reducir este tipo de riesgo, los profesionales de Seguridad utilizarían el principio de disponibilidad, así como las directrices organizativas basadas en marcos para garantizar que los miembros del personal solo puedan acceder a los datos que necesitan para realizar su trabajo.