**La relación entre los marcos y los controles**

* **Marcos y controles**

Los **marcos de seguridad** son directrices que se utilizan para elaborar planes que ayuden a mitigar los riesgos y las amenazas para los datos y la privacidad. Los marcos apoyan la capacidad de las organizaciones para adherirse a las leyes y Regulaciones de Cumplimiento. Por ejemplo, el sector sanitario utiliza marcos para cumplir la Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA) de Estados Unidos, que exige que los profesionales médicos mantengan a salvo la información de los pacientes.

* **Controles**

Los **controles** de seguridad son salvaguardas diseñadas para reducir riesgos de seguridad *específicos*. Los controles de seguridad son las medidas que utilizan las organizaciones para reducir el Riesgo y las amenazas a los Datos y a la Privacidad. Por ejemplo, un control que puede utilizarse junto con los marcos para garantizar que un hospital sigue cumpliendo la HIPAA es exigir que los pacientes utilicen la autenticación de múltiples factores (MFA) para acceder a sus registros médicos. Utilizar una medida como la MFA para validar la identidad de alguien es una forma de ayudar a mitigar los riesgos potenciales y las amenazas a los datos privados.

**Marcos y controles específicos**

Existen muchos marcos y controles diferentes que las organizaciones pueden utilizar para seguir cumpliendo la normativa y alcanzar sus objetivos de Seguridad. Los marcos cubiertos en esta lectura son el Marco de Ciberamenazas (CTF) y la Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27001. También se explican varios Controles de seguridad comunes, utilizados junto con estos tipos de marcos.

**Marco de la Amenaza Cibernética (CTF)**

Según la Oficina del director de Inteligencia Nacional, el CTF fue desarrollado por el gobierno de EE.UU. para proporcionar "un lenguaje común para describir y comunicar información sobre la actividad de las ciberamenazas" Al proporcionar un lenguaje común para comunicar información sobre la actividad de las amenazas, el CTF ayuda a los profesionales de la ciberseguridad a analizar y compartir información de forma más eficaz. Esto permite a las organizaciones mejorar su respuesta al panorama de la ciberseguridad en constante evolución y a las numerosas tácticas y técnicas de los agentes de amenazas.

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

Un framework internacionalmente reconocido y utilizado es ISO/IEC 27001. La familia de Estándares ISO 27000 permite a las organizaciones de todos los sectores y tamaños gestionar la seguridad de los recursos, como la información financiera, la Propiedad intelectual, los datos de los empleados y la información confiada a terceros. Este framework esboza los requisitos para un sistema de gestión de la Seguridad de la información, las mejores prácticas y los controles que apoyan la capacidad de una organización para gestionar los riesgos. Aunque el framework ISO/IEC 27001 no requiere el uso de controles específicos, sí proporciona una colección de controles que las organizaciones 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 a la Seguridad, riesgo o vulnerabilidad. Los controles pueden ser físicos, técnicos y administrativos y suelen utilizarse para prevenir, detectar o corregir problemas de Seguridad.

Ejemplos de controles físicos:

* Puertas, vallas y cerraduras
* Guardias de seguridad
* Circuito cerrado de televisión (CCTV), cámaras de vigilancia y detectores de movimiento
* Tarjetas de acceso o distintivos para entrar en los espacios de oficina

Ejemplos de controles técnicos:

* Firewalls
* MFA
* Software antivirus

Ejemplos de controles administrativos:

* Separación de funciones
* Autorización
* Clasificación de activos

**Puntos clave**

Los marcos y controles de Ciberseguridad se utilizan conjuntamente para establecer la postura de Seguridad de una organización. También apoyan la capacidad de una organización para alcanzar los objetivos de Seguridad y cumplir con las leyes y regulaciones. Aunque estos frameworks y controles suelen ser voluntarios, se recomienda encarecidamente a las organizaciones que los implementen y utilicen para ayudar a garantizar la seguridad de los recursos críticos.