Marcos de seguridad

Son directrices utilizadas para crear planes que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad, proporcionan un enfoque estructurado para implementar el ciclo de vida de seguridad, el cual 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 con las normativas. Tienen distintos propósitos

* Proteger la PII
* Asegurar la información financiera
* Identificar las debilidades de seguridad
* Administras los riesgos organizacionales
* Alinear la seguridad con los objetivos comerciales

Los marcos, poseen cuatro componentes principales

1. Identificar y documentar los objetivos de seguridad
2. Establecer directrices para lograr los objetivos de seguridad
3. Implementación de procesos de seguridad solidos
4. Monitoreo y comunicación de resultados

**Controles de seguridad:** son medidas de seguridad diseñadas para reducir los riesgos de seguridad específicos. Esto, junto con los marcos es vital para administrar la seguridad de todos los tipos de organizaciones y garantizar que todos hagan su parte para mantener un nivel de riesgo bajo

**Triada CID**

Es un modelo fundamental que ayuda a informar como las organizaciones consideran el riesgo al establecer sistemas y políticas de Seguridad, CID es sinónimo de confidencialidad, integridad y disponibilidad

**• Confidencialidad:** solo los usuarios autorizados tienen acceso a activos o datos específicos

**•Integridad:** los datos son correctos, auténticos y confiables, esto se puede generar gracias a la encriptación por ejemplo

**•Disponibilidad:** los datos son accesibles para quienes están autorizados a acceder a ellos

**•Recurso:** es un elemento que se percibe como valioso para una organización

**Marco de ciberseguridad de NIST:** marco de cumplimiento voluntario que consiste en estándares, directrices y mejores practicas para gestionar el riesgo de ciberseguridad, es la base para gestionar los riesgos a corto y largo plazo

**Comisión Federal Reguladora de la Energía - Corporación Norteamericana de Fiabilidad Eléctrica (FERC-NERC)**

La FERC-NERC es una normativa que se aplica a las organizaciones que trabajan con electricidad o que están relacionadas con la red eléctrica de Estados Unidos y Norteamérica. Este tipo de organizaciones tienen la obligación de prepararse, mitigar y notificar cualquier posible incidente de seguridad que pueda afectar negativamente a la red eléctrica. También tienen la obligación legal de adherirse a las Normas de Fiabilidad para la Protección de Infraestructuras Críticas (CIP) definidas por la FERC.

**Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP®)**

FedRAMP es un programa del gobierno federal de EE.UU. que estandariza la evaluación de la seguridad, la autorización, la supervisión y la gestión de los servicios en la nube y las ofertas de productos. Su objetivo es proporcionar coherencia entre el sector gubernamental y los proveedores de nube de terceros.

**Centro para la Seguridad en Internet (CIS®)**

Es una organización sin animo de lucro con múltiples áreas de interés, proporciona un conjunto de controles que pueden utilizarse para salvaguardar sistemas y redes contra ataques. Su objetivo es ayudar a establecer un mejor plan de defensa en las organizaciones, además, proporciona controles procesables que los profesionales de la seguridad pueden seguir si se produce un incidente de seguridad

**Reglamento General de Protección de Datos (RGPD)**

Es un reglamento general de datos de la Unión Europea que protege el tratamiento de los datos de los residentes en la UE y su derecho a la privacidad dentro y fuera del territorio de la UE

**Estándar de seguridad de los datos para la industria de tarjetas de pago (PCI DSS)**

Es una norma de seguridad internacional destinada a garantizar que las organizaciones almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hacen en un entorno seguro

**Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)**

Es una ley federal estadounidense establecida en 1996 para proteger la información sanitaria de los pacientes, esta prohíbe que la información de los pacientes se comparta sin su consentimiento, se rige por 3 normas  
1- Privacidad

2- Seguridad

3- Notificación de infracciones

Además de conocer la ley HIPAA, los profesionales de la seguridad deben estar familiarizados con la Health Information Trust Alliance (HITRUST®), que es un marco de seguridad y un programa de garantía que ayuda a las instituciones a cumplir la ley HIPAA.

**Organización Internacional de Normalización (ISO)**

Se creo para establecer normas internacionales relacionadas con la tecnología, la fabricación y la gestión transfronterizas, ayuda a las organizaciones a mejorar sus procesos y procedimientos de retención de personal, planificación, residuos y servicios

**Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)**

El consejo de normas de auditoría del American Institute of Certified Public Accountants® (AICPA) desarrolló esta norma. Los SOC1 y SOC2 son una serie de informes que se centran en las políticas de acceso de los usuarios de una organización a diferentes niveles organizativos como:

* Asociado
* Supervisor
* Gerente
* Ejecutivo
* Proveedor
* Otros

Se utilizan para evaluar el cumplimiento financiero y los niveles de riesgo de una organización. También abarcan la confidencialidad, privacidad, integridad, disponibilidad, seguridad y protección general de los datos. Los fallos de control en estas áreas pueden conducir al fraude.

**Principios éticos en la ciberseguridad**

* *Confidencialidad*: para analizarla desde la parte ética, podemos ejemplar que si usted encuentra información privada como la PII o la SPII, su trabajo es mantener esa información confidencial y segura
* *Protección de la privacidad*: significa proteger la información personal del uso no autorizado
* *La ley*: las leyes son reglas reconocidas por una comunidad y aplicadas por una entidad gubernamental