### ****Semana 1: Dominios de seguridad****

**Son 8 dominios de seguridad identificados por el CISSP.**

Loa 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

**Dominio de seguridad y gestión de riesgos.** Tiene varias de enfoque:Definir metas y objetivos de seguridad las organizaciones pueden reducir los riesgos para activos críticos y datos críticos 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 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.

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.

Como profesional de la seguridad se debe seguir las reglas y expectativas de comportamiento ético, para minimizar la negligencia el abuso o el fraude

**Dominio:** **Seguridad de activos** es asegurar los activos digitales (PII y SPII ) y físicos. También se relaciona con almacenar, mantener, conservar, destruir datos físicos y virtuales.

PII y SPII deben ser manejados y protegidos de forma segura ya sea en un almacenen digital, se transfieran por una red como Internet, o incluso que se recopilen físicamente.

Se debe tener políticas y procedimientos que garanticen que los datos se almacenen, mantengan, conserven y destruyan correctamente.

Saber que datos hay y quien accede a ellos es necesario para tener una fuerte postura de seguridad que mitigue los riesgos contra los activos críticos y los datos.

Supervisar la destrucción correcta de discos duros esto garantiza que no se acceda a los datos

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. 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 de arquitectura y diseño de seguridad**. 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.

Estos procesos son creados por quienes se dedican a la arquitectura e ingeniería de seguridad.

Esto es en base a una responsabilidad compartida en que todos en una compañía 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

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 de seguridad de las comunicaciones y de las redes.** Se trata de la gestión y protección de la 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

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 permanezca segura cuando sus empleados/as viajan o trabajan fuera de la oficina principal.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

**Dominio de Gestión de identidad y acceso (IAM)** Se centra en el acceso y autorización para proteger los datos asegurándose de que los usuarios sigan las políticas de control y manejo de activos.

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.

Se tiene que limitar el acceso a lo que los empleados necesitan, el IAM reduce el riesgo general para los sistemas y datos, es decir 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.

Ejemplo: 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.

Se debe evitar usar el mismo inicio de sesión de administrador ya que no habría forma de saber quien tiene acceso a que datos, y en caso de una falla de seguridad es imposible separar la actividad de usuario valida la de los agentes de amenaza

IAM tiene 4 componentes principales:

* **Identificación:** Verifica quien es brindando un nombre de usuario, una tarjeta de acceso o datos biométricos como una huella dactilar.
* **Autentificación:** Es el proceso de verificar la identidad de alguien mediante una contraseña o pin
* **Autorizacion:** Se da tras confirmar la identidad del usuario y su nivel de acceso depende del puesto en la organizacion
* **Responsabilidad:** Se refiere al monitoreo y registro de las acciones de los usuarios como los inicio de sesión para demostrar que los sistemas y datos se utilizan adecuadamente

**Dominio de evaluación y pruebas de seguridad** se centra en realizar pruebas de control de seguridad, recopilar y analizar datos y realizar auditorias de seguridad para monitorear riesgos amenazas y vulnerabilidades, con estas pruebas se identifican nuevas formas y mejores formas de mitigar amenazas, riesgos y vulnerabilidades.

Las organizaciones pueden emplear pruebas de penetración, un proceso conocido como pentesting, para encontrar vulnerabilidades que podría aprovechar un agente de amenaza.

Implementar autentificación de varios factores

Pruebas de control de la seguridad, y que recopilen y analicen datos.

Auditar los permisos de usuarios/as, a fin de confirmar si tienen los niveles correctos de acceso a los sistemas internos.

**Dominio de las operaciones de seguridad** Se centra en realizar investigaciones e implementar medidas preventivas. Esto a raíz de un incidente 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.

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.

Una vez neutralizada la amenaza se empieza a recopilar evidencia e datos digitales y físicos para llevar a cabo una investigación forense digital, esto para identificar cuando, 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

Por medio 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.

En este dominio trabajan en equipo para gestionar, prevenir e investigar amenazas, riesgos y vulnerabilidades. En este dominio trabajan en equipo para gestionar, prevenir e investigar amenazas, riesgos y vulnerabilidades. Una vez identificada una amenaza, el equipo trabaja para mantener a salvo los datos y la información privada.

**Dominio de** **Seguridad en el desarrollo de software** Centrado en prácticas de codificación segura, que son las pautas recomendadas para crear aplicaciones y servicios seguros. Uso de prácticas y políticas de programación para crear aplicaciones seguras.

Cada fase del siclo de vida del desarrollo se somete a revisiones de seguridad ya que la seguridad se integra por completo en el producto.

Revisión de diseño seguro, durante la fase de diseño. Revisiones de código seguro durante las fases de desarrollo y prueba, así como con pruebas de penetración durante la fase de implementación y despliegue aseguran que la seguridad se integre en el producto de software.

Realizar pruebas de seguridad de las aplicaciones puede ayudar a garantizar que las vulnerabilidades sean identificadas y mitigadas adecuadamente.

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.

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.

--------------------------------------------------------------------------------------------------------------------------------

Importante sabe que: Debe haber una vulnerabilidad y una amenaza para que haya un riesgo.

Capacitar a los empleados:

Identificar correo posible de phishing es un buen inicio.

Usar tarjetas de acceso para los empleados.

Se debe mejorar los esfuerzos para identificar y mitigar vulnerabilidades y mitigar las amenazas y los riesgos.

**Ransomware:** Es un ataque malicioso que se encripta los datos de una organización y exigen un pago para restaurar el acceso.

Puede trabajar los sistemas de red y dejar los dispositivos inutilizables y encriptar y bokear datos confidenciales, blokeando así el acceso a los dispositivos

La web esta compuesta por tres capas:

1. **Web superficial.** La usa la mayoría acceso rápido desde el navegador
2. **Depp web.** Suele requerir autorización para acceder a ella ejemplo una intranet de una compañía, ya que solo acceden colaboradores o personas autorizadas
3. **Dark web.** Solo se puede acceder mediante un software especial

Tres impactos clave de amenazas, riesgos y vulnerabilidades.

**El primero** es el impacto financiero, cuando los activos se ven comprometidos por un ataque como malware, las consecuencias financieras pueden ser significativas por varias razones: pueden incluir interrupción de la producción y los servicios esto trae costos muy altos para solucionar esto además de multas si los activos se ven comprometidos por el incumplimiento de las leyes y regulaciones.

**El segundo** impacto es el robo de identidad ya que las organizaciones almacenan datos privados de clientes, empleados y proveedores, (PII y SPII) tener estos datos es un riesgo para las empresas que pueden ser vendidos o filtrados a través de la dark web esto ocurre porque la dark web ofrece una sensación de secretismo y los agentes de amenaza venden los datos ahí sin consecuencias legales

**El tercero** es el daño a la reputación de una organización. Una solida base de clientes apoya la misión de la organización su visión y sus objetivos financieros. Si se aprovecha una vulnerabilidad los clientes pueden buscar nuevas relaciones comerciales con competidores o crear mala publicidad que daña la reputación de la organización.

Pereder datos de clientes no solo afecta a la reputación de la organización y sus finanzas si no que puede generar sanciones y multas.

Los 7 puntos del Marco de Gestión de Riesgos del NIST

Una amenaza habitual son las configuraciones erróneas y solicitar acceso a algo que no es necesario.

Se debe tener buenas políticas de gestión de dispositivos, el trabajo en equipo y la buena comunicación con otros equipos es primordial

### ****2: Marcos y controles de seguridad****

El Instituto Nacional de Estándares y tecnología (NIST) ofrece muchos marcos utilizados por profesionales de seguridad, para manejar riesgos, amenazas y vulnerabilidades.

NIST y Marco de Gestión de Riesgos (RMF)

Tener una comprensión solida de como mitigar y manejar los riesgos, puede diferenciarte de otros candidatos.

**Marco de Gestión de Riesgos tiene 7 pasos:**

**Preparar**: Se refiere a las actividades necesarias para gestionar los riesgos de seguridad y privacidad antes de que ocurra una falla de seguridad. Monitoreo e identificar controles para reducirlos

**Categorizar:** Sirve para desarrollar procesos y tareas de manejo de riesgos, tareas en como la confidencialidad, integridad y disponibilidad de los sistemas e información que pueden verse afectados. Entender los procesos establecidos por la organización para reducir riesgos

**Seleccionar:** Es elegir, personalizar y capturar la documentación de los controles que protegen a una organización. Ejemplo actualizar un manual de procedimientos o gestionar otra documentación que permitan abordar problemas de forma mas eficiente

**Implementar:** Planes de seguridad y privacidad para la organización, tener buenos planes para minimizar el impacto de riesgos de seguridad continuos

**Evaluar:** Se refiere a determinar si los controles establecidos se implementaron correctamente. Una organización siempre requiere operar con la máxima eficiencia posible, por esto se tiene que analizar si los procedimientos y controles que se implementaron cumple con las necesidades de la organización. Se tienen que identificar debilidades y determinar si las herramientas, procedimientos, controles y protocolos de la organización deben cambiarse para gestionar mejor los riesgos

**Autorizar:** Significa ser responsable de los riesgos de seguridad y privacidad que pueden existir en una organización, esto significa generar informes, desarrollar planes de acción y establecer hitos del proyecto que estén alineados con los objetivos de seguridad de la organización

**Monitorear:** Es estar al tanto de como operan los sistemas. Evaluar y mantener las operaciones técnicas son tareas diarias de un analista. Parte de mantener un nivel bajo de riesgo para una organización es saber como los sistemas actuales apoyan objetivos de seguridad de la organización. Si los sistemas no satisfacen los objetivos pueden necesitarse cambios. Hay que asegurarse de que los procedimientos establecidos funcionen como deben a fin de minimizar riesgos para la organización y sus usuarios

La ciberseguridad implica proteger a las organizaciones y a las personas de amenazas, riesgos y vulnerabilidades.

Brindar a las organizaciones la posibilidad de diseñar políticas y procesos que ayuden  a prevenir y mitigar este tipo de problemas de seguridad

# Gestiona amenazas, riesgos y vulnerabilidades comunes

**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**

¿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 es proteger sus activos

Un **activo** es un elemento que se percibe como valioso para una organización.( puede ser digital o físico)

**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.

Activos físicos:

* Terminales de pago.
* Servidores.
* Computadoras de escritorio.
* Espacios de oficina.

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)** <https://csrc.nist.gov/projects/risk-management/about-rmf>

**del Instituto Nacional de Estándares y Tecnología (NIST)**

<https://csrc.nist.gov/projects/risk-management/about-rmf>

**y la Health Information Trust Alliance (HITRUST).**

<https://hitrustalliance.net/hitrust-framework?utm_term=&utm_campaign=HITRUST_i1_PaidSearch&utm_source=adwords&utm_medium=ppc&hsa_acc=2724012343&hsa_cam=16641331914&hsa_grp=136906352837&hsa_ad=598980848547&hsa_src=g&hsa_tgt=dsa-1659695676388&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQiAorKfBhC0ARIsAHDzsluRN5tSpCQal-rYnZLo2wUNppQdUHUba82LMX3JMGOoRPEJ6wG6-LgaAryYEALw_wcB>

## Amenazas, riesgos y vulnerabilidades más comunes

**Amenaza** es cualquier circunstancia o evento que puede afectar negativamente a los activos.

Con un nivel inicial, tu trabajo consiste en ayudar a preservar los activos de la organización frente a amenazas internas y externas.

Amenazas comunes:

**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.**

**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.

* **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](https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/cybersecurity-risks).

<https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/cybersecurity-risks>

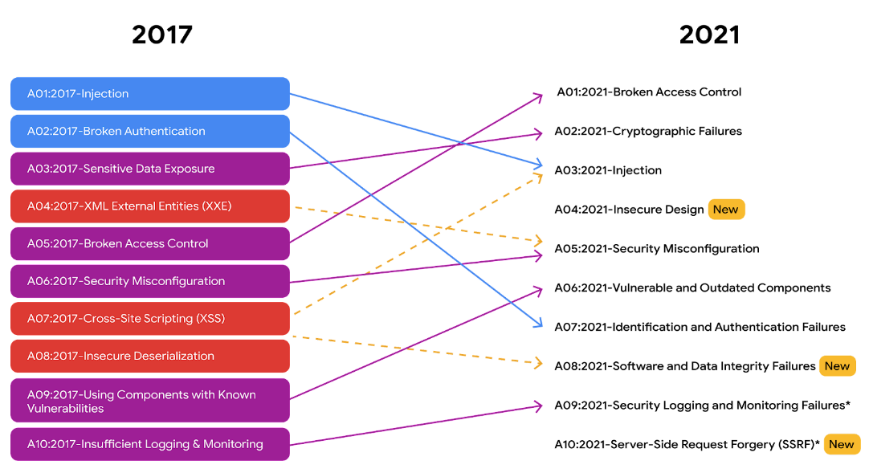
Además, el Open Web Application Security Project (OWASP) publica un documento estándar de concientización sobre los [10 riesgos de seguridad más críticos](https://owasp.org/www-project-top-ten/)

https://owasp.org/www-project-top-ten/

para las aplicaciones web, que se actualiza regularmente.

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.

**­**

****

Una **vulnerabilidad** es una debilidad que puede ser aprovechada por una amenaza.

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.

**Gestión de vulnerabilidades**, consiste en monitorear un sistema para identificarlas y mitigarlas. Aunque existan parches y actualizaciones, si no se aplican, pueden producirse intrusiones.

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.

OWASP Top Ten

<https://owasp.org/www-project-top-ten/>

**NIST RMF**

<https://csrc.nist.gov/projects/risk-management/about-rmf>

**Establecer planes de protección contra amenazas, riesgos y vulnerabilidades**

**Para esto se usan los marcos de trabajo como punto de partida para crear políticas y procesos de seguridad**

**Un marco de seguridad son pautas usadas para crear planes, para mitigar riesgos y amenazas contra los datos y la privacidad, como ataques de ingeniería social y ransomware.**

**La seguridad va mas allá del espacio virtual, también incluye el espacio físico**

**Otros marcos de seguridad indican como prevenir detectar y responder a las fallas de seguridad.**

**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 así mismo, educar a los empleados sobre los desafíos de ciberseguridad es esencial para minimizar la posibilidad de una filtración, reconocer señales de alarma y amenazas potenciales es esencial, así como disponer de planes para reportar y abordar problemas rápidamente.**

**Un analista comprende e implementar los planes que haya preparado para proteger a la organización sus empleadores y usuarios contra ataques de ingeniería social, fallas y otros incidentes de seguridad**

**Mientras que los marcos se usan 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 falsa de empleados o proporcionar beneficios gratuitos .**

**Los controles son medidas de protección diseñadas para reducir riesgos específicos.**

**Se analizarán tres tipos comunes de controles:**

1. **Cifrado: Proceso de convertir datos de un formato legible a un formato codificado, el texto cifrado es el mensaje codificado en bruto, es ilegible para humanos y computadoras, el cifrado se utiliza para confidencialidad de datos sensibles, como la información de cuentas o números de seguro social**
2. **Autenticación: Protege datos sensibles y se refiere a verificar la identidad de alguien o algo. Esto significa iniciar sesión con un usuario y una contraseña, existen métodos de autenticación de múltiples factores (MFA) someten al usuario a demostrar que es quien dice ser requiriendo una contraseña y un formulario extra de autentificación como un código de seguridad o datos biométricos como huella dactilar, voz o verificación facial. La biometría se refiere a características físicas únicas que pueden usarse para verificar identidades: escaneo ocular, huella dactilar o palma de la mano.**

**Vishing es un ejemplo de ataque de ingeniería social que aprovecha los datos biométricos, es el aprovechamiento de la comunicación electrónica de voz para obtener información sensible para hacerse pasar por una fuente conocida. Vishing podría usarse para suplantar la voz de una persona y robar su identidad para cometer un delito.**

1. **Autorización: Es el concepto de conceder acceso a recursos específicos dentro de un sistema, se utiliza para verificar que una persona tiene permiso para acceder a un recurso.**

**Los controles de seguridad son solo un elemento de una gía de seguridad conocida como la tríada CID esta se usa para proteger a las organizaciones**

**Como se vinculan los marcos y los controles**

Marco de Gestión de Riesgos (RMF)

Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST)

La tríada de confidencialidad, integridad y disponibilidad (CID)

## 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:

Brindan soporte a las organizaciones para acatar las leyes y las normas de cumplimiento.

Los **controles de seguridad:** Son medidas de protección diseñadas para reducir riesgos de seguridad específicos, son utilizadas por las organizaciones para disminuir los riesgos y amenazas a los datos y la privacidad.

Una medida de control que se puede usar junto con los marcos de seguridad para garantizar que el cumplimiento de una ley, regulación o norma de seguridad.

Existen diversos marcos y controles que las organizaciones pueden utilizar para cumplir con las regulaciones y alcanzar sus objetivos de seguridad:

### ****Marco de Amenaza Cibernética (Cyber Threat Framework, 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****

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.

**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.

**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

**Controles técnicos:**

* Cortafuegos (firewalls)
* Autenticación de múltiples factores (MFA)
* Software de antivirus

**Controles administrativos:**

* Separación de funciones
* Autorización
* Clasificación de activos

**La tríada CID es un modelo que ayuda a las organizaciones a evaluar los riesgos y configurar sistemas y políticas de seguridad.**

**C = confidencialidad: Solo los usuarios autorizados tienen acceso a ciertos activos o datos.**

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.

**I = integridad: Implica que los datos sean correctos, auténticos y confiables .**

Es esencial contar con protocolos para verificar la autenticidad de los datos y una manera de hacerlo es mediante la criptografía <https://www.nist.gov/cryptography#:~:text=Cryptography%20uses%20mathematical%20techniques%20to,that%20drives%20research%20and%20innovation>.

se utiliza para transformar los datos, para que las partes no autorizadas no puedan leerlos ni manipularlos

Otro ejemplo es mediante la activación del cifrado, que es el proceso de convertir los datos de un formato legible a uno codificado

**D = disponibilidad: Implica que solo puedan acceder a los datos quienes tengan autorización.** Cuando un sistema cumple tanto los principios de disponibilidad como los de confidencialidad, los datos pueden ser utilizados cuando sea necesario.

**Estos son los 3 principios básicos al proteger a la organización y sus usuarios**

Diseñar sistemas y políticas con estos elementos en mente ayuda a establecer una **postura de seguridad** exitosa, 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

**Marcos del Nacional de estándares y Tecnología (NIST)**

**Creados por los EEUU.**

**Los marcos son usados como punto de partida para crear planes que mitiguen riesgos, amenazadas y vulnerabilidades contra datos y activos sensibles.**

**Existen organizaciones que crean marcos que los profesionales de ciberseguridad pueden usar para desarrollar esos planes esto incluye empresas con o sin fines de lucro,asi como agencias gubernamentales.**

**Marco de ciberseguridad (CSF) del (NIST)**

**Incluye estándares pautas y mejores prácticas para manejar los riesgos de ciberseguridad, es muy respetado y esencial para mantener la seguridad independientemente de donde trabajes.**

**Se usa para prevenir amenazas, riesgos y vulnerabilidades.**

**Es un marco que principalmente se usa para desarrollar planes para manejar incidentes, de forma correcta y rápida y reducir el riesgo, así proteger contra una amenaza y mitigar posibles vulnerabilidades.**

**Ofrece un marco unificado para proteger los sistemas de información dentro del gobierno federal.**

**Cuenta con protección de EEUU en la publicación especial: del NIST S.P.800-53**

**Los controles de este marco se usan para mantener la tríada CID de esos sistemas usados por el gobierno, así marcos y controles funcionan de forma conjunta.**

**Comprender SP 800-53 del NIST es clave si te interesa trabajar para EEUU**

**Sus ventajas son:**

**El CSF consta de 5 funciones importantes:**

1. **Identificar: Se relaciona con la gestión de riesgos monitoreo de dispositivos para saber cuáles están comprometidos**
2. **Proteger: Mediante la implementación de políticas, procedimientos, capacitaciones y herramientas que ayudan a mitigar las amenazas de ciberseguridad, esto se aplica frente amenazas y ataques nuevos y desconocidos. Estudiar datos históricos y mejorar las políticas y procedimientos es esencial.**
3. **Detectar: Es identificar posibles incidentes de seguridad y mejorar las capacidades de monitoreo, para aumentar la velocidad y eficiencia de las detecciones. También como analista el trabajo será recopilar y organizar datos a fin de documentar un incidente y sugerir mejoras en los procesos para evitar que se repita**
4. **Responder: Es tomar las medidas adecuadas para contener, neutralizar y analizar los incidentes de seguridad e implementar mejoras en el proceso de seguridad**
5. **Recuperar: Es restaurar la operación normal de los sistemas afectados, datos y activos como archivos financieros o legales después de un incidente, lo más rápido posible**

**Cada función puede utilizarse para mejorar la seguridad con medidas de formas proactivas y reactivas, por eso estas 5 funciones son esenciales.**

**Estos ayudan a gestionar los riesgos de ciberseguridad, implementar estrategias de gestión y aprender de errores anteriores, estas funciones son claves para proteger una organización: contra amenazas, riesgos y vulnerabilidades potenciales.**

**Principios y auditorias de seguridad OAWASP**

**Hay principios y pautas marcos NIST y tríada CID para ayudar a los equipos a minimizar amenazas y riesgos.**

**Open Web Application Security Project (OAWASP)**

**El primer principio es minimizar el área de superficie de ataque, esto se refiere a toda vulnerabilidad potenciales que un agente de amenaza puede aprovechar, como vectores de ataque que son: correo phishing y contraseñas poco seguras**

**Para minimizar la superficie de ataque se puede desactivar funciones del software, restringir quien puede acceder a ciertos activos o establecer requisitos de contraseña mas complejos**

**El primer principio del privilegio mínimo significa que los usuarios tengan el menor nivel de acceso necesario para realizar sus tareas diarias la razón de esto se limita el acceso a la información y los recursos de la organización es para reducir el daño que podría causar una violación de seguridad. De esta manera si una cuenta esta comprometida, pero tiene acceso limitados será menor el impacto de los daños puesto que al carecer de privilegios no puede realizar un ataque mayor.**

**El primer principio defensa en profundidad esto implica tener varios controles de seguridad que aborden los riesgos y amenazas de distintas maneras, como la autentificación de múltiples factores, firewoks, sistemas de detección de intrusiones.**

**El primer principio la separación de funciones se realiza para evitar que la gente lleve a cabo actividades fraudulentas o ilegales. Nadie debe recibir tantos privilegios que pueda abusar del sistema. Ejemplo: Quien firma las nóminas debe de estar separado del que las prepara.**

**El primer principio es simplificar la seguridad Esto al implementar controles de seguridad deben evitarse soluciones innecesariamente complejas, esto ya que pueden ser difíciles de gestionar ya que mientras mas complejo sean los controles de seguridad será más difícil trabajar en colaboración**

**El primer principio es corregir correctamente los problemas de seguridad cuando ocurre un incidente de seguridad se espera identificar la causa principal rápidamente, aquí la importancia de corregir cualquier vulnerabilidad identificadas, es bueno realizar pruebas de seguridad para asegurar que las reparaciones sean exitosas una contraseña débil del wifi podría causar una falla de seguridad para solucionar esto se implementan políticas de contraseñas más estrictas.**

## Otros principios de seguridad de OWASP

**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**

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. 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 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.

Para estar al día de las tendencias s de ciberseguridad es consultar foros en línea como Medium para saber más de los temas de ciberseguridad. Medium es fácil por el uso de filtrado por etiquetas sobre artículos de interés esto revisando los foros.

Una auditoria de ciberseguridad se utiliza para revisar que tan seguro son los controles políticas y procedimientos que tiene una organización.

Existen 2 principales auditorias de seguridad: externas y internas.

Auditoria interna la realiza un equipo puede incluir: Un encargado de cumplimiento o gerente de seguridad estas se realizan para mejorar la postura de seguridad de una organización y evitar multas en una agencia reguladora, por falta de cumplimiento normativo, estas identifican riesgos, evalúa los controles y corrige problemas de cumplimiento.

**Una auditoria debe de tener en su planificación:**

1. **Definición de alcance y los objetivos**
2. **Evaluación de riesgo de los activos**
3. **Evaluar los controles**
4. **Evaluar el cumplimiento**
5. **Y comunicar los resultados a las partes interesadas.**

Antes de realizar la redacción por escrito de la auditoria **se tiene que cuestionar lo siguiente:**

**¿Qué se quiere lograr con la auditoria?**

**¿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 debe implementar?**

Estas preguntas dan una base para evaluar los controles esto 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.

**Definición de alcance son los criterios de una auditoria interna este requiere identificar las personas, activos, políticas, procedimientos y tecnologías que podrían afectar a la postura de seguridad.**

**Definición de objetivos son un planteo de las metas de seguridad o que se quiere lograr, para mejorar la postura de seguridad.**

**Ejemplo:**

**1.-Alcance:**

**Evaluar los permisos del usuario.**

**Identificar los controles políticas y procedimientos actuales.**

**Tener en cuenta la tecnología utilizada actualmente en la organización.**

**1.-Objetivos:**

**Implementar funciones centrales de los marcos como CSF del NIST**

**Definir políticas y procedimientos para garantizar el cumplimiento normativo**

**Fortalecer los controles del sistema**

**2.-Evaluar el riego**

**Esto se centra en identificar amenazas, riesgos y vulnerabilidades potenciales, esto ayuda a las organizaciones a decidir que medidas de seguridad implementar y monitorear para proteger sus activos, se evalúa la falta del manejo de una forma adecuada de activos físicos y digitales incluidos los equipos del personal. El equipo usado para almacenar datos no está bien protegido.**

**Puede destacarse si se está implementando controles, procesos y procedimientos inadecuados para proteger los activos, mencionar si hace falta un manejo adecuado de activos y digitales incluidos los equipos del personal**

**para ver qué tipos de controles y normativa de cumplimiento se necesita tener para mejorar la postura de la seguridad**

**3.- Evaluar los controles**

**Se tienen que clasificar los controles en las siguientes categorías**:Controles administrativos técnicos y físicos.

**Controles administrativos:** Se relacionan con el componente humano de la ciberseguridad, estos son políticas y procedimientos que definen como una organización gestiona los datos ejemplo: Las políticas de contraseñas

**Controles técnicos:** Son soluciones de hardware y software, para proteger los activos como usar sistemas de intrusiones (IDS) y cifrado

**Controles físicos.** Son medidas implementadas para evitar el acceso físico a los activos protegidos como cámaras de vigilancia y cerraduras

**4.-** **El siguiente paso es corroborar si la organización sigue o no el cumplimiento normativo** estas reglas normativas se refieren a las leyes que la organización debe seguir para proteger los datos privados. Un ejemplo de esto si una empresa acepta pagos con tarjetas, por lo tanto, debe cumplir con el RGPD y los estándares de seguridad de datos del sector de las tarjetas de pago.

**5.- Comunicar los resultados, así como las recomendaciones a las partes interesadas**

**Resume el alcance y los objetivos de la auditoria**

**Enumera los riesgos existentes e indica con que velocidad deben abordarse**

**Identificar el cumplimiento normativo que la organización debe seguir**

**Dar recomendaciones**

**Las auditorías internas permiten identificar vulnerabilidades dentro de la organización.**

**Ejemplo: En una auditoria de contraseñas puede dar como resultado que muchas eran poco seguras, una vez que se identificó el problema, esto dio la pauta para crear políticas de contraseña más estrictas, por lo tanto, las auditorias permiten determinar que medidas de seguridad hay y que áreas deben mejorarse para lograr la postura de seguridad deseada.**

**Las auditorias son complejas pero aportan mucho valor a la organización**

### ****3.- Introducción a las herramientas de ciberseguridad****

### ****4.- Uso de los manuales de estrategias para responder a incidentes****