### ****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.

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 y destruir datos.

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

**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. 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

**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

**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.

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

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.

Implementar autentificación de varios factores

**Dominio de las operaciones de seguridad** Se centra en realizar investigaciones e implementar medidas preventivas. Esto a raíz de un incidente de seguridad, este proceso requiere una mayor urgencia para minimizar los riesgos potenciales contra la organización si hay un ataque aactivo 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 acabo una investigación forense digital, esto par identificar cuando, como y por que se produjo la falla con esto los equipos de seguridad definen áreas de mejora y medidas preventivas para mitigar futuros ataques

**Dominio de** **Seguridad en el desarrollo de software** centrado en practicas de codificación segura, que son las pautas recomendadas para crear aplicaciones y servicios seguros. 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, asi como con pruebas de penetración durante la fase de implementación y despliegue aseguran que la seguridad se integre en el producto de software

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

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

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