**Dominios CISSP**

Los equipos de seguridad los utilizan para organizar las tareas diarias e identificar las brechas en la seguridad que podrían causar consecuencias negativas para una organización y para establecer su *postura de seguridad* la cual se refiere a la capacidad de una organización para gestionar su defensa de los activos y datos críticos y reaccionar ante los cambios, como lo mencionamos antes, hay 8 dominios:

1. Gestión de seguridad y riesgos: hay varias áreas de interés para este dominio:   
   - Definición de metas y objetivos de seguridad: esto ayuda a reducir los riesgos para los recursos y datos críticos como la PII  
   - Mitigación de riesgos: disponer de los procedimientos y normas adecuados para reducir rápidamente el impacto de un riesgo como una violación  
   - Cumplimiento normativo: método principal utilizado para desarrollar las políticas de seguridad internas de una organización, los requisitos reglamentarios y las normas independientes  
   - Continuidad del negocio: este caso se refiere a la capacidad de una organización para mantener su productividad diaria mediante el establecimiento de planes de recuperación ante desastres por riesgos  
   - Regulaciones legales: cumplir con las leyes
2. Seguridad de los activos: se centra en proteger los activos digitales y físicos, a su vez, se relaciona con el almacenamiento, mantenimiento, retención y destrucción de datos. Esto significa que recursos tales como la PII o la SPII deben manejarse de forma segura y protegerse, tanto si se almacenan en una computadora, se transfieren a través de una red como Internet o incluso si se recogen físicamente, también se necesita contar con políticas y procedimientos que garanticen que los datos se almacenan, mantienen, conservan y destruyen correctamente. Saber qué datos se tienen y quién tiene acceso a ellos es necesario para tener una postura de seguridad solida que mitigue el riesgo para los recursos y datos críticos
3. Arquitectura de seguridad y la ingeniería: se centra en optimizar la seguridad de los datos garantizando que existen herramientas, sistemas y procesos eficaces para proteger los recursos y los datos de una organización. Uno de los conceptos centrales de la arquitectura de diseño seguro es la *Responsabilidad compartida*, la cual significa que todas las personas de una organización asumen un papel activo en la reducción del riesgo y en el mantenimiento de la seguridad tanto física como virtual
4. Seguridad de las comunicaciones y las redes: busca gestionar y proteger las redes físicas y las comunicaciones inalámbricas. Las redes seguras mantienen a salvo los datos y las comunicaciones de una organización ya sea in situ, en la nube o cuando se conecta a servicios de forma remota
5. Gestión de identidad y acceso: esta centrada en el acceso y la autorización para mantener los datos seguros asegurándose de que los usuarios siguen las políticas establecidas para controlar y gestionar los activos. Su objetivo es reducir el riesgo global para los sistemas y los datos
6. Evaluación y pruebas de seguridad: se basa en realizar pruebas de control de la seguridad, la recopilación y el análisis de datos y la realización de auditorias de seguridad para supervisar los riesgos, las amenazas y las vulnerabilidades. Las pruebas de controles de seguridad pueden ayudar a una organización a identificar nuevas y mejores formas de mitigar las amenazas, los riesgos y las vulnerabilidades. Esto implica examinar las metas y objetivos de la organización y evaluar si los controles que se están utilizando realmente logran esas metas. Recopilar y analizar datos de seguridad regularmente también ayuda a prevenir amenazas y riesgos para la organización.
7. Operaciones de seguridad: se centra en realizar investigaciones e implementar medidas preventivas. Las investigaciones comienzan una vez que se ha identificado un incidente de seguridad, requiere un mayor sentido de la urgencia para minimizar los riesgos potenciales para la organización. Si hay un ataque activo, mitigar el ataque y evitar que siga escalando es esencial para garantizar que la información privada está protegida de los agentes de amenaza. Una vez neutralizada la amenaza, comenzará la recopilación de pruebas digitales y físicas para llevar a cabo una investigación forense. Debe llevarse a cabo una investigación forense digital para identificar cuándo, cómo y por qué se produjo la brecha.
8. Seguridad en el desarrollo de software: busca el uso de practicas de programación seguras, ya que son directrices recomendadas que se utilizan para crear aplicaciones y servicios seguros. El ciclo de vida de desarrollo de software es un proceso eficiente utilizado por los equipos para crear rápidamente productos y funciones de software. En este proceso, la seguridad es un paso adicional. Al garantizar que cada fase del ciclo de vida de desarrollo de software se somete a revisiones de seguridad, la seguridad puede integrarse completamente en el producto de software.

**Amenaza:** cualquier circunstancia o evento que pueda afectar negativamente a los activos, como un ataque de ingeniería social. Las amenazas mas comunes incluyen:

* **Amenazas internas:** miembros del personal o proveedores que abusan de su acceso autorizado para obtener datos que pueden perjudicar a una organización
* **Amenazas persistentes avanzadas:** un agente de amenaza que mantiene el acceso no autorizado a un sistema durante un largo periodo de tiempo

**Riesgo:** cualquier cosa que pueda afectar a la confidencialidad, la integridad o la disponibilidad de un recurso, es decir, la probabilidad de que ocurra una amenaza, son calificados en diferentes niveles:

* Bajo
* Medio
* Alto

Hay diferentes factores que peuden afectar a la probabilidad de un riesgo para los recursos de una organización, entre ellos:

* Riesgo externo: cualquier cosa fuera de la organización que tenga el potencial de dañar los recursos de la organización, como un agente de amenaza intentado acceder a información privada
* Riesgo interno: un empleado actual o anterior, un proveedor o socio de confianza que suponga un riesgo
* Sistemas heredados: sistemas antiguos que podrían no estar contabilizados o actualizados, pero igual pueden tener un impacto en los recursos
* Riesgo multiparte: externalizar el trabajo a proveedores externos puede darles acceso a la propiedad intelectual
* Cumplimiento normativo/licencias de software: software que no esta actualizado o en conformidad, o parches que no se instalan a tiempo

También se pueden calificar según las posibles amenazas y valor de un *recurso*

**Recurso de bajo riesgo:** información que no perjudicaría la reputación de la organización ni las operaciones en curso, y que no causaría daños financieros si se viera comprometida, como información pública o datos publicados

**Recurso de riesgo medio:** puede incluir información que no esta disponible para el público y puede causar algún daño a las finanzas, la reputación o las operaciones en curso de la organización, como la publicación anticipada de las ganancias trimestrales que podría afectar las acciones

**Recurso de alto riesgo:** cualquier información protegida por reglamentos o leyes que, si se pone en peligro, tendría un impacto negativo grave en las finanzas, como una filtración de SPII o propiedad intelectual

Algunas estrategias comunes utilizadas para gestionar los riesgos incluyen:

* Aceptación: aceptar un riesgo para evitar que se interrumpa la continuidad del negocio
* Evitación: creación de un plan para evitar el riesgo por completo
* Transferencia: transferencia del riesgo a un tercero para que lo gestione
* Mitigación: disminuir el impacto de un riesgo conocido

**Vulnerabilidad:** debilidad que puede ser aprovechada por una amenaza, para que exista un riesgo, tanto una vulnerabilidad como una amenaza deben estar presentes, algunos ejemplos de vulnerabilidad son: firewall o una aplicación desactualizada, contraseñas débiles, etc. Las personas también pueden ser una vulnerabilidad, ya que sus acciones pueden afectar significativamente a la red interna de una organización

**Ransomware:** ataque malicioso en el que los actores encriptan los datos de una organización y luego exigen un pago para restaurar el acceso

Las amenazas, los riesgos y las vulnerabilidades, poseen tres tipos de impactos:

1. Impacto financiero: cuando los recursos se ven comprometidos por un ataque, como el uso de software malicioso, las consecuencias financieras pueden ser significativas, como la interrupción de la producción y los servicios o el coste de corregir el problema
2. Robo de identidad: las organizaciones deben decidir si almacenan datos privados de clientes, empleados y proveedores externos, y durante cuánto tiempo. Almacenar cualquier tipo de datos sensibles supone un riesgo para la organización. Los datos sensibles pueden incluir información de identificación personal, o PII, que puede venderse o filtrarse a través de la web oscura. Esto se debe a que la web oscura proporciona una sensación de secretismo y los agentes de amenaza pueden tener la capacidad de vender datos allí sin enfrentarse a consecuencias legales.
3. Daño a la reputación de una organización: cuando una vulnerabilidad es explotada, puede llevar a los clientes a buscar nuevas relaciones comerciales con la competencia o crear mala prensa que cause un daño permanente a la reputación de una organización. La pérdida de datos de clientes no solo afecta a la reputación y finanzas de una organización, también puede dar lugar a sanciones legales y multas

En el *Marco de Gestion de Riesgos* existen 7 pasos:

1. Preparar: se refiere a las actividades que son necesarias para gestionar los riesgos de seguridad y privacidad antes de que se produzca una violación
2. Categorizar: se utiliza para desarrollar procesos y tareas de gestión de riesgos. Luego, los profesionales de seguridad utilizan esos procesos y desarrollan tareas pensando en como el riesgo puede afectar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información
3. Seleccionar: seleccionar medios para elegir, personalizar y capturar la documentación de los controles que protegen a una organización, como mantener un manual de estrategias actualizado
4. Implementar planes de seguridad y privacidad para la organización: disponer de buenos planes es esencial para minimizar el impacto de los riesgos de seguridad actuales
5. Evaluar: determinar si los controles establecidos se implementan correctamente
6. Autorizar: significa ser responsable de los riesgos de seguridad y privacidad que puedan existir en una organización, lo que implicaría la generación de informes, el desarrollo de planes de acción y establecimiento de hitos del proyecto
7. Monitorear: significa estar al tanto de como funcionan los sistemas, la evaluación y el mantenimiento de las operaciones técnicas son tareas que los analistas realizan a diario