Definición de Ciberseguridad y Seguridad Computacional

- Ciberseguridad: de acuerdo con Amazon Web Service (AWS), la ciberseguridad es una metodología o práctica de proteger equipos (ya sea a nivel de software o hardware), sistemas críticos y datos de posibles amenazas digitales. En la ciberseguridad se utilizan medidas y herramientas en el cual protegen datos confidenciales del acceso no autorizado o de intrusiones, así también como para evitar interrupciones de operaciones empresariales debido a actividades no deseadas
- Seguridad computacional: disciplina que aplica controles físicos, técnicos y administrativos para proteger la confidencialidad, integridad y disponibilidad de los activos digitales y los sistemas que los procesan (Pfleeger & Pfleeger, 2023).

Tríada CIA (Confidencialidad – Integridad – Disponibilidad)

- Qué significa cada componente y ejemplos básicos.
- **Confidencialidad** – la confidencialidad trata sobre los esfuerzo y desempeño que toma una compañía para que sus datos más sensibles no queden al ojo público o más bien queden totalmente privados. Esto implica, como componente clave, en que se tenga un sistema configurado con listas de control de acceso, en el cual permita que un grupo de usuario no puedan acceder a dichos datos o información privilegiada.
- Por ejemplo, aquellos que trabajan con las finanzas de una organización deben poder acceder a las hojas de cálculo, cuentas bancarias y otra información relacionada con el flujo de dinero. Sin embargo, es posible que no se otorgue acceso a la gran mayoría de empleados, y quizás incluso a ciertos ejecutivos. Para garantizar que se sigan estas políticas, deben existir restricciones estrictas para limitar quién puede ver qué.
- Integridad – La integridad trata en asegurar que los datos estén completamente seguros y sin alteraciones. La integridad de los datos se mantiene solo si estos son auténticos, precisos y confiables. La integridad de los datos puede verse comprometida tanto de forma intencional como accidental. En algunos casos, un atacante logra evadir los sistemas de detección de intrusos (IDS), modifica archivos para abrir accesos no autorizados o manipula registros del sistema con el fin de encubrir su actividad y debilitar la seguridad de la información. Por otro lado, también pueden ocurrir errores involuntarios, como ingresar un código incorrecto o realizar acciones descuidadas. Incluso, si la organización no cuenta con políticas, controles y procedimientos adecuados, la integridad puede deteriorarse sin que haya una acción directa por parte de algún individuo.

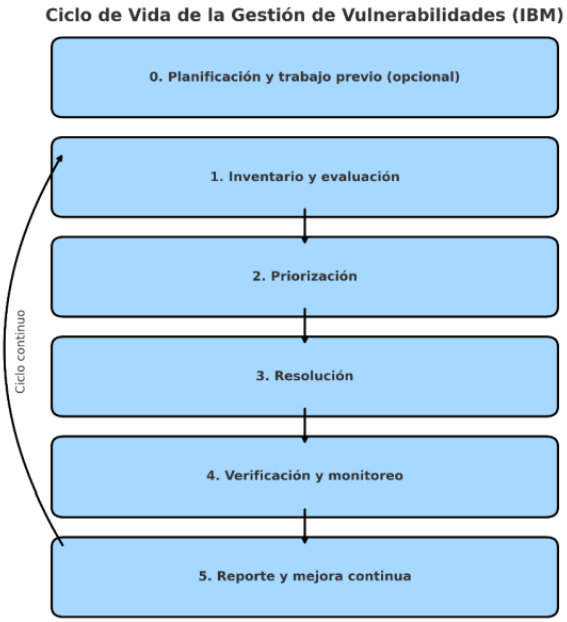
- Ejemplo: si su empresa proporciona información sobre gerentes sénior en su sitio web, esta información debe tener integridad. Si es impreciso, las personas que visitan el sitio web para obtener información pueden sentir que su organización no es confiable.
- Disponibilidad - La disponibilidad es la capacidad de acceder a los datos y recursos cuando se necesitan. Aunque la confidencialidad y la integridad de la información se mantengan intactas, los datos resultan inservibles si no están disponibles para los usuarios autorizados en el momento adecuado. Esto implica que los sistemas, redes y aplicaciones deben operar correctamente y de manera continua. Además, quienes tienen permiso para acceder a cierta información deben poder consultarla sin demoras excesivas, garantizando así la eficiencia en las operaciones tanto internas como en el servicio al cliente.
- Por ejemplo, si ocurre un apagón y no existe un plan de recuperación ante desastres, los usuarios podrían perder el acceso a sistemas esenciales, lo que pondría en peligro la disponibilidad. Asimismo, fenómenos naturales (Acts of God) como inundaciones o fuertes tormentas de nieve pueden impedir que los empleados lleguen a sus lugares de trabajo, afectando el uso de estaciones y equipos necesarios para acceder a información o aplicaciones críticas. La disponibilidad también puede verse afectada por ataques intencionales, como los ataques de denegación de servicio (DoS) o infecciones por ransomware, que buscan interrumpir el acceso a los recursos.

Métodos de Análisis de Riesgo

- Cuantitativo: Método de evaluación que mide el riesgo en valores numéricos concretos, generalmente expresados en dinero o probabilidad porcentual. Permite lo que sería el cálculo de pérdidas económicas.
- Ejemplo: “El riesgo de ransomware es de $2,000,000 en pérdidas esperadas”
- Cualitativo: Método de evaluación que clasifica el riesgo de forma descriptiva o categórica (Alto, Medio, Bajo) sin necesidad de números exactos.
- Ejemplo: “El riesgo de phishing es ALTO porque los empleados no están entrenados”.

Ciclo de Vida de la Gestión de Vulnerabilidades

- Etapas principales: Inventario y evaluación, Priorización, Resolución, Verificación y monitoreo, Reporte y mejora continua. Este es el diagrama de la lección 2 del Módulo1



Amenazas Maliciosas Dirigidas

- **Dirigidas (Targeted)**
- **Spear-Phishing:** Es una variante del phishing, pero mucho más dirigida y personalizada. Mientras que el phishing normal manda correos masivos a miles de personas, el spear-phishing apunta a una persona específica o a un grupo reducido dentro de una organización.
- Ejemplo:
    - ✓ Un atacante sabe que eres gerente de finanzas.
    - ✓ Te envía un correo que parece venir de tu jefe directo, pidiéndote aprobar una transferencia urgente con un enlace a un sistema falso.
    - ✓ Como está tan bien personalizado, aumenta la probabilidad de que caigas en la trampa.
- **APT contra infra-crítica:**
    - **Caracteristicas:**
        - Lo realizan grupos organizados (hackers patrocinados por Estados o crimen organizado).
        - Avanzado: usan herramientas sofisticadas (malware a medida, exploits 0-day).
        - Persistente: permanecen ocultos en la red durante meses o años.

        - Threat (amenaza): buscan objetivos estratégicos, no ataques masivos al azar.

- Infra-Crítica (Infraestructura Crítica): Se refiere a los sistemas esenciales de un país o empresa, cuya caída impactaría en la sociedad o economía.
    - Ejemplos:
        - Redes eléctricas.
        - Plantas de agua potable.
        - Hospitales.
        - Banca y telecomunicaciones.
        - Transporte (aeropuertos,trenes).
- Un APT contra Infra-Crítica es un ataque sofisticado y persistente llevado a cabo contra una infraestructura crítica, con el fin de Espiar (robo de información sensible), Sabotear (interrupción de servicios esenciales) e Infligir daño económico, social o incluso militar.
    - Ejemplo: Stuxnet (2010):
        - APT que atacó sistemas SCADA (Supervisory Control and Data Acquisition) en plantas nucleares de Irán.
        - Alteró centrifugadoras para dañarlas físicamente.
        - Considerado el primer “ciberarma” contra infra-crítica