UNIDAD 1. INTRODUCCIÓN A LA CIBERSEGURIDAD

Actividad 1. Empecemos con lo básico

Jose Francisco Ochoa Ornelas

225396812

1. Ciberseguridad

Definición

La **Ciberseguridad** (o seguridad digital) es el conjunto de prácticas, tecnologías, procesos y controles diseñados para **proteger** sistemas, redes, programas, dispositivos e información digital de ataques, daños, accesos no autorizados o uso indebido, asegurando la **Confidencialidad**, **Integridad** y **Disponibilidad** de los activos digitales.

Características Clave

- **Se enfoca en lo digital:** Su alcance se limita a la protección de datos y activos en formato electrónico (sistemas, redes, aplicaciones).
- **Prevención y Respuesta:** Incluye medidas proactivas (prevención) y capacidad de reacción (detección y respuesta rápida) ante incidentes.
- **Pilares fundamentales:** Se basa en la triada C-I-A (Confidencialidad, Integridad y Disponibilidad).

Dato Importante

Según informes de 2024, en México se registraron **más de 187 mil millones de intentos de ciberataques**, lo que lo posiciona como uno de los países más atacados en Latinoamérica, evidenciando el crecimiento acelerado y la persistencia de las amenazas digitales.

2. Seguridad de la Información (InfoSec)

Definición

La **Seguridad de la Información (InfoSec)** es un término más amplio que se define como la protección de la **información importante** (activos de información) contra el acceso, la divulgación, el uso, la alteración, la destrucción o la interrupción no autorizados, **independientemente de su formato** (digital o físico, como papel).

Características Clave

- **Alcance amplio:** Cubre información en todos sus formatos (digital, impreso, verbal) y medios (físico, lógico y humano).
- **Pilares esenciales:** Se rige por la tríada C-I-A:
    - **Confidencialidad:** Proteger la información sensible contra el uso no autorizado (ej. cifrado, control de acceso).
    - **Integridad:** Garantizar que la información sea precisa, completa y no haya sido alterada sin autorización.
    - **Disponibilidad:** Asegurar que los sistemas y datos estén accesibles para los usuarios autorizados cuando los necesiten (ej. copias de seguridad, redundancia).
- **La Ciberseguridad es un subcampo:** La seguridad informática/ciberseguridad es una parte de la InfoSec que se centra en los datos digitales.

Dato Importante

La tríada de la CIA (Confidencialidad, Integridad y Disponibilidad) es la **piedra angular** de cualquier programa de seguridad de la información, sirviendo como los principios guía para implementar controles y políticas de protección.

3. Vulnerabilidad

Definición

Una **Vulnerabilidad** en ciberseguridad es una **debilidad, fallo o error** en un sistema, aplicación, red, hardware o proceso (incluyendo el factor humano) que puede ser **explotada** por una amenaza para comprometer la seguridad y causar un daño.

Características Clave

- **Debilidad intrínseca:** Es una falla existente en el activo (no es una acción).
- **Explotabilidad:** Es la capacidad de que la debilidad sea aprovechada por un atacante.
- **Tipos comunes:** Pueden ser de software (errores de código, falta de parches), de hardware (defectos de diseño), de configuración (permisos deficientes) o humanas (error, falta de capacitación).

Dato Importante

Las organizaciones de ciberseguridad realizan **pruebas de penetración** y **análisis de vulnerabilidades** de forma proactiva para detectarlas y corregirlas (aplicar un "parche") antes de que un atacante malintencionado las explote.

4. Amenaza

Definición

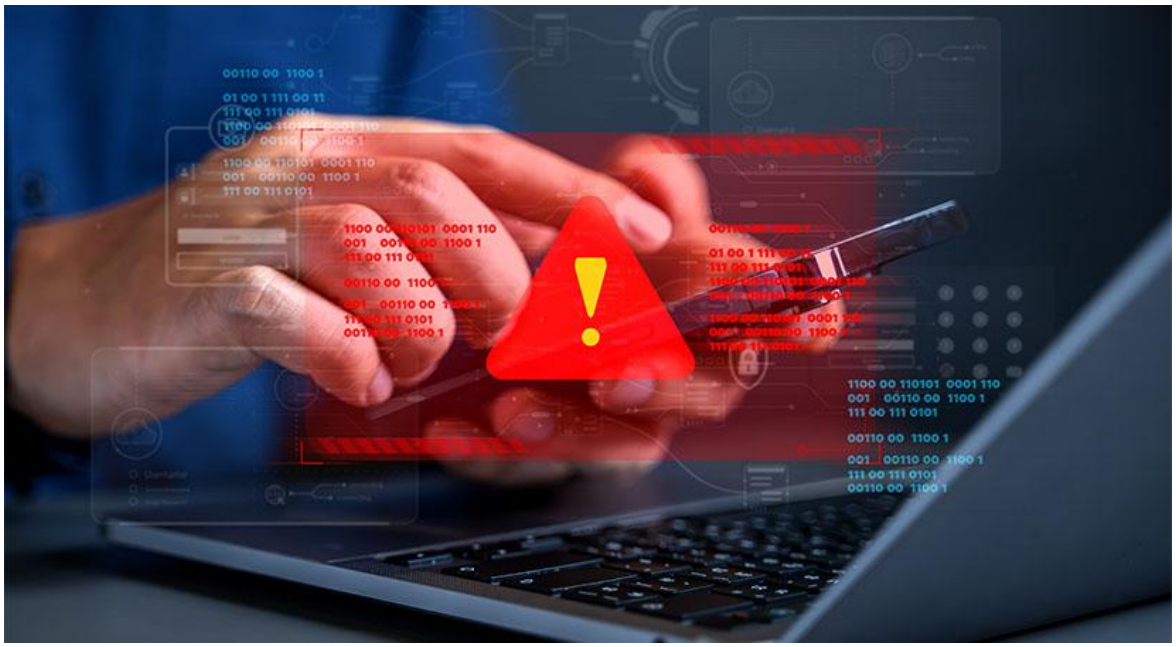
Una **Amenaza** es un evento o acción con el **potencial de causar un daño** a un sistema o a la información, aprovechando una vulnerabilidad para comprometer la Confidencialidad, Integridad o Disponibilidad de los activos. Es la **causa** potencial de un incidente no deseado.

Características Clave

- **Origen:** Puede ser intencional (actor malicioso, hacker, ciberdelincuente) o accidental (error humano, desastre natural).
- **Necesita un vector:** Se materializa a través de un **vector de ataque** (ej. correo de *phishing*, *malware*).
- **Evolutiva:** Las amenazas avanzan al ritmo de la tecnología, requiriendo una adaptación constante de las defensas.

Dato Importante

El **Phishing** (suplantación de identidad por correo electrónico o mensajes) es una de las **formas de ciberataque más comunes** y efectivas, porque explota la vulnerabilidad humana (falta de concienciación) en lugar de un fallo técnico.



5. Riesgo

Definición

El **Riesgo** de ciberseguridad es la **probabilidad** de que una amenaza se materialice explotando una vulnerabilidad, y el **impacto** potencial o las consecuencias negativas que resultan de ese evento (pérdida de datos, pérdidas económicas, daño a la reputación, etc.).

Riesgo ≈ Probabilidad (Amenaza) × Impacto (Consecuencia)

Clasificaciones

Los riesgos de ciberseguridad se pueden clasificar de varias maneras:

1. Basados en la Consecuencia (Tipo de Daño)

- **Riesgo de Pérdida de Datos/Información:** Ocurre por accidentes, fallos técnicos o ataques que resultan en la destrucción o indisponibilidad de la información.
- **Riesgo de Fuga de Información (Filtración):** Divulgación no autorizada de datos sensibles (incumpliendo la Confidencialidad).
- **Riesgo de Acceso No Autorizado:** El ciberatacante obtiene credenciales o acceso a sistemas sin permiso.
- **Riesgo de Interrupción de Operaciones:** El sistema o servicio deja de funcionar (incumpliendo la Disponibilidad).

2. Basados en el Origen de la Amenaza

- **Riesgos Técnicos:** Relacionados con fallas de *software*, *hardware* o configuración (ej. *malware*, inyección SQL).
- **Riesgos Humanos:** Relacionados con el personal (ej. error de un empleado, ataque de ingeniería social).
- **Riesgos Ambientales/Físicos:** Afectaciones por desastres naturales o fallas de seguridad física (ej. inundación, robo de equipos).

Dato Importante

La **Gestión de Riesgos** es un proceso continuo que implica **identificar** los activos, **evaluar** las amenazas y vulnerabilidades, **priorizar** los riesgos y **aplicar medidas correctivas** (controles de seguridad) para reducir la probabilidad o el impacto a un nivel aceptable.

---

6. Seguridad y 7. Protección

En el contexto de la ciberseguridad y seguridad de la información, estos términos se utilizan a menudo de forma intercambiable o estrechamente relacionada.

Seguridad (General)

Definición

El estado de **estar libre de peligro o riesgo**. En el ámbito tecnológico, se refiere al objetivo de mantener los activos y la información a salvo de daños.

Características Clave

- **Estado ideal:** Es la condición que se busca lograr para los sistemas y la información (estar protegido).
- **Marco de acción:** Implica la implementación de políticas, procedimientos y estándares.

Protección (General)

Definición

Se refiere a las **medidas, herramientas o acciones concretas** que se toman para **evitar** que ocurra un daño. En ciberseguridad, se habla de soluciones de *protección* de puntos de conexión (*antivirus*, *firewalls*).

Características Clave

- **Acción proactiva:** Implica la aplicación de controles para prevenir incidentes.
- **Ejemplos de medidas:** Cifrado, autenticación multifactor (MFA), copias de seguridad, firewalls.

Dato Importante

Un **programa de ciberseguridad efectivo** combina **Seguridad** (el estado de estar protegido, definido por políticas) y **Protección** (las herramientas y acciones para lograr ese estado). Un ejemplo de medida de protección es la adopción del modelo de **Confianza Cero** (*Zero Trust*), que asume que nadie dentro o fuera de la red debe ser confiable por defecto y exige verificación continua.

Referencias

Ciberseguridad y Seguridad de la Información

Akamai. (s.f.). *¿Qué es la ciberseguridad o seguridad cibernética?* Recuperado de https://www.akamai.com/es/glossary/what-is-cybersecurity

Amazon Web Services (AWS). (s.f.). *¿Qué es la ciberseguridad?* Recuperado de https://aws.amazon.com/es/what-is/cybersecurity/

Fundación Sadosky. (2023). *Seguridad de la información y ciberseguridad*. Recuperado de https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

Vulnerabilidad y Amenaza

Check Point Software. (s.f.). *Las 6 principales amenazas a la ciberseguridad*. Recuperado de https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

Check Point Software. (s.f.). *Las 8 principales vulnerabilidades en ciberseguridad*. Recuperado de https://www.checkpoint.com/es/cyber-hub/cyber-security/top-8-cyber-security-vulnerabilities/

Hewlett Packard Enterprise (HPE). (s.f.). *¿Qué es una amenaza de ciberseguridad?* Recuperado de https://www.hpe.com/mx/es/what-is/cybersecurity-threats.html

Riesgo, Seguridad y Protección

SMOWL. (2024). *Vulnerabilidad en la seguridad informática: qué es, definición, tipos y consejos*. Recuperado de https://smowl.net/es/blog/vulnerabilidad-en-la-seguridad-informatica/