# Ciberseguridad

# *Glosario de términos*

James Edward Nuñez Cuzcano

2ºDAW 2025/26

Ultima modificación 12/11/2025

# Indice

## *Bloque 1 – Amenazas y vulnerabilidades informáticas*

Amenaza: Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Cifrar: Cifrar es transformar información legible en un formato incomprensible mediante algoritmos y claves, para protegerla de accesos no autorizados y garantizar su confidencialidad.

Confidencialidad: La confidencialidad en seguridad informática es el principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización. Dicha autorización se basa en la necesidad de conocer la información para el desempeño de su actividad y se debe proveer tanto para la información almacenada como la información en tránsito.

Cross-Site Scripting (XSS): Un Cross-Site Scripting (XSS) es un ataque que inyecta código malicioso en páginas web, permitiendo ejecutar scripts en el navegador de la víctima para robar datos, secuestrar sesiones o manipular contenido.

DdoS: Una denegación de servicio distribuida (Distributed Denyal of Service) es un DoS realizado desde múltiples máquinas controladas (botnet), lo que aumenta la intensidad del ataque y complica su mitigación.

Disponibilidad: Capacidad de un sistema, servicio o recurso para estar accesible y operativo para usuarios autorizados cuando lo necesiten (incluye redundancia, tolerancia a fallos y recuperación ante interrupciones).

DoS: Una denegación de servicio (Denyal of Service) es un ataque que deja un servicio inaccesible para usuarios legítimos al agotar

sus recursos (ancho de banda, CPU o conexiones) desde una única fuente.

Exploit: Un exploit es un código, herramienta o técnica que aprovecha una vulnerabilidad para ejecutar acciones no autorizadas en un sistema.

Ingeniería social: La ingeniería social es una técnica de manipulación psicológica dirigida a engañar a personas para obtener información, credenciales o que realicen acciones que comprometan la seguridad (ej.: phishing, pretexting, tailgating).

Integridad: La integridad informática establece que los datos o información son exactos y fiables y que no han sido modificados por terceros no autorizados.

Inyección SQL: Una inyección SQL es un ataque que inserta código malicioso en consultas SQL para acceder, manipular o borrar datos de una base de datos sin autorización.

Man-in-theMiddle: Un ataque Man-in-the-Middle es una intrusión en la que un atacante intercepta y/o altera la comunicación entre dos partes sin que ellas lo sepan, para espiar, robar credenciales o manipular datos.

Malware: Un malware es un software malicioso diseñado para dañar, espiar, robar información o tomar control de sistemas; incluye virus, troyanos, gusanos, ransomware y spyware.

Ransomware: Un ransomware es un malware que bloquea o cifra los archivos de un sistema y exige un pago a la víctima para restaurar el acceso a la información.

Vulnerabilidad: Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

## *Bloque 2 – Medidas de protección básicas*

Auditoría: Una auditoría es un examen sistemático de sistemas, redes o procesos para evaluar su seguridad, cumplimiento de normas y detectar vulnerabilidades o riesgos.

Autenticación Multifactor (MFA): La autenticación multifactor (MFA) es un método de verificación que requiere dos o más factores (algo que sabes, algo que tienes o algo que eres) para confirmar la identidad de un usuario.

Filtrado: El filtrado es un mecanismo que controla y selecciona el tráfico de información en una red o sistema, permitiendo o bloqueando datos según reglas de seguridad definidas.

Firewall: Un firewall es un software de seguridad que controla y filtra el tráfico permitiendo o bloqueando conexiones según reglas definidas, puede ser de dos tipos, local si esta instalado en el cliente, en cuyo caso filtra el trafico de este equipo o de red si esta instalado en el router, en cuyo caso filtra el trafico que entra y sale de la red.

Monitoreo: El monitoreo es la supervisión continua de sistemas, redes o aplicaciones para detectar anomalías, fallos o incidentes de seguridad y garantizar su correcto funcionamiento.

Permisos: Un permiso es una autorización que define las acciones que un usuario o rol puede realizar sobre un recurso en un sistema, como leer, modificar o eliminar.

Puerto: Un puerto es un punto de comunicación en un dispositivo de red que permite enviar y recibir datos entre aplicaciones o servicios a través de protocolos específicos.

Protocolo: Un protocolo es un conjunto de reglas y estándares que define cómo se transmiten, reciben y procesan los datos entre dispositivos o aplicaciones en una red, garantizando comunicación correcta y segura.

Reglas: Una regla en un firewall es una instrucción que determina si un tráfico de red específico debe permitirse o bloquearse según criterios como dirección IP, puerto o protocolo.

Roles: Un rol es un conjunto de permisos y responsabilidades asignados a un usuario o grupo dentro de un sistema para controlar el acceso a recursos y funciones.

Router: Un router es un software que se encarga de interconectar varias redes locales y redirigir entre estas el trafico de red entre estas.

## *Bloque 3 – Análisis de los incidentes de seguridad*

Análisis forense: El análisis forense en ciberseguridad es el proceso de investigar, recolectar y examinar evidencias digitales de sistemas, redes o dispositivos para determinar cómo ocurrió un incidente, quién lo causó y qué información fue afectada. Su objetivo es reconstruir los eventos de manera precisa y preservar la integridad de la evidencia para posibles acciones legales o correctivas.

El análisis forense permite no solo entender un ataque, sino también mejorar defensas y prevenir incidentes futuro.

Ciclo de vida de un incidente:

- **Detección:** Identificar señales o alertas de que algo anormal ocurre en sistemas, redes o aplicaciones. Incluye monitoreo, logs y reportes de usuarios.
- **Análisis:** Investigar el incidente para determinar su origen, alcance, gravedad y posibles afectados. Permite planificar las acciones correctivas.
- **Contención:** Aplicar medidas inmediatas para limitar el impacto, evitando que el incidente se propague o cause más daños. Puede ser temporal o estratégica.
- **Erradicación:** Eliminar la causa raíz del incidente, como malware, vulnerabilidades o accesos no autorizados, para asegurar que no vuelva a ocurrir.
- **Recuperación:** Restaurar sistemas, servicios y datos a un estado seguro y funcional, asegurando que operen normalmente sin riesgos residuales.
- **Aprendizaje:** Documentar todo el incidente, analizar fallos y aciertos, y actualizar políticas, procedimientos y controles de seguridad para prevenir futuros incidentes.

Estrategias proactivas: Las estrategias proactivas en ciberseguridad son medidas y prácticas anticipadas que buscan prevenir incidentes antes de que ocurran, en lugar de solo reaccionar una vez que se detecta un ataque. Estas estrategias implican identificar riesgos potenciales, fortalecer sistemas y procesos, y reducir las oportunidades de que un atacante logre comprometer la seguridad.

Incluyen acciones como:

- **Gestión de vulnerabilidades:** escanear y actualizar software regularmente para cerrar fallas de seguridad.
- **Pruebas de penetración:** simular ataques controlados para identificar debilidades antes de que los atacantes reales las exploten.
- **Segmentación de redes:** dividir la red en zonas para limitar el alcance de un posible ataque.
- **Políticas de seguridad y concienciación:** capacitar a usuarios y definir normas claras para minimizar errores humanos y riesgos de ingeniería social.
- **Implementación de controles de acceso estrictos:** usar autenticación multifactor y permisos basados en roles para proteger información sensible.

Estas estrategias permiten a las organizaciones reducir riesgos, detectar amenazas tempranas y mantener la resiliencia de sus sistemas frente a posibles ataques.

Incidente de seguridad: Un incidente de seguridad es cualquier evento que amenaza la integridad, confidencialidad o disponibilidad de sistemas, datos o servicios, como ataques, fallos o accesos no autorizados.

Indicadores de compromiso (IoC): Un indicador de compromiso es cualquier evidencia técnica que sugiere que un sistema, red o aplicación ha sido comprometido por un ataque o actividad maliciosa. Los IoC pueden incluir archivos maliciosos, cambios inesperados en configuraciones, tráfico de red anómalo, registros de eventos sospechosos, intentos de acceso no autorizados, conexiones a servidores externos controlados por atacantes o presencia de malware. Su análisis permite identificar brechas de seguridad, confirmar incidentes, responder rápidamente y fortalecer las defensas para prevenir futuros ataques.

## *Bloque 4 – Herramientas y tecnologías de aplicación*