Espacio curricular: **TIC**

Docente: Emiliano Jeremias Suárez

Cursos: 5to Año A y B

Horas cátedras semanales: 6HRS

Turno: Mañana

Año: 2026

Clase 33°
Ciberseguridad, definición y conceptos

La ciberseguridad es la práctica técnica, operativa y estratégica de proteger sistemas, redes, dispositivos y datos contra accesos no autorizados, ataques digitales e interrupciones del servicio. Se fundamenta en modelos teóricos de gestión de riesgos y arquitecturas defensivas de múltiples capas.

Conceptos clave identificados:

1. **La Tríada CIA (Confidencialidad, Integridad y Disponibilidad): El modelo teórico pilar sobre el que se diseña cualquier sistema seguro:**

- ***Confidencialidad:*** **Garantizar que la información sea accesible únicamente por entidades autorizadas (mediante cifrado, gestión de claves y control de acceso).**
- ***Integridad:*** **Asegurar la autenticidad y precisión de los datos, previniendo su alteración no autorizada (mediante funciones hash, firmas digitales y sumas de verificación).**
- ***Disponibilidad:*** **Garantizar el acceso continuo a los sistemas e información para los usuarios legítimos (mediante redundancia, políticas de respaldo y mitigación de ataques DDoS).**

2. **Modelo Zero Trust ("No confiar nunca, verificar siempre"): Cambio de paradigma propuesto originalmente por Forrester y estandarizado por el NIST. Elimina la "confianza implícita" dentro del perímetro de la red corporativa, exigiendo autenticación continua, control de acceso de menor privilegio (*Least Privilege Access*), microsegmentación y cifrado de extremo a extremo en cada solicitud de tráfico.**
3. **Defensa en Profundidad (*Defense-in-Depth*): Estrategia que implementa múltiples capas superpuestas de seguridad (red, endpoint, aplicaciones, identidad y datos) para garantizar que, si un atacante vulnera una capa, las capas adyacentes contengan la brecha.**
4. **Taxonomía de Amenazas y Arquitectura:**
    - ***Vulnerabilidad vs. Exploit:*** **Una vulnerabilidad es una debilidad en el código o diseño del sistema; un exploit es la técnica o script diseñado para aprovechar esa debilidad.**
    - ***Gestión de Identidades y Accesos (IAM) y MFA:*** **Sistemas para autenticar y autorizar identidades mediante factores múltiples (biometría, tokens, credenciales).**
    - ***Endpoint Detection and Response (EDR):*** **Herramientas avanzadas que supervisan los dispositivos finales de la red para detectar y contener comportamiento anómalo en tiempo real.**

¿Cuál es la diferencia entre VULNERABILIDAD y Exploit?

En el lenguaje mas adolescente, por ejemplo, se utiliza mucho el termino Exploit puede ser una técnica, código o conjunto de herramientas que una persona con intenciones maliciosas desarrolla e implementa para poder aprovechar una vulnerabilidad en el sistema.

En cambio una vulnerabilidad, podría decirse que es una debilidad, fallo o deficiencia en la configuración de un sistema o infraestructura de la misma. Permitiendo esto buscar e intentar buscarle una falla a ese sistema, juego, aplicación, etc. Para permitir un acceso o uso no autorizado.

Trabajo Practico 33°

1) **En base a lo explicado en clase, leído en este PDF. ¿Qué es un malware?**
2) **¿Qué tipo de malware existen?**
3) **¿Qué es taxonomía?**