PRINCIPIOS FUNDAMENTALES

SEGURIDAD INFORMATICA

CIA TRIAD (TRIADA DE SEGURIDAD)

Confidencialidad
Protege la información del acceso no autorizado. Se implementa con:

- *Cifrado de datos*
- *Autenticación multifactor (MFA)*
- *Políticas de acceso restrictivo*

Integridad
Garantiza que la información no sea alterada sin autorización. Se logra mediante:

- Firmas digitales
- Control de versiones
- Mecanismos de hash (SHA-256, MD5)

Disponibilidad
Asegura que los datos y sistemas estén accesibles cuando se necesiten. Se mantiene con:

- Copias de seguridad
- Sistemas redundantes
- Protección contra ataques DDoS

PRINCIPALES AMENAZAS

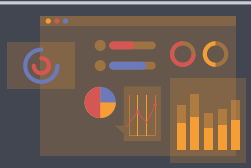
Malware (Software Malicioso)
Virus, ransomware, troyanos que dañan sistemas y roban información.

Phishing
Correos o mensajes fraudulentos que engañan a usuarios para robar credenciales.

Ataques DDoS
Sobrecarga de tráfico en servidores para inhabilitar servicios en línea.

VULNERABILIDADES COMUNES

- Software desactualizado (Falta de parches de seguridad)
- Contraseñas débiles (Uso de combinaciones fáciles de adivinar)
- Redes inseguras (Falta de cifrado en conexiones WiFi públicas)



ISO 27001

- Define un sistema de gestión de seguridad de la información.
- Enfocado en políticas, procedimientos y controles.

NORMATIVAS INTERNACIONALES

ISO 27002

- Guía práctica con medidas de seguridad recomendadas.
- Complementa la implementación de la ISO 27001.

NORMATIVAS INTERNACIONALES