



Fundamentos de Ciberseguridad y Hacking Ético  
Una defensa activa en la era digital

## Introducción

- Vivimos en un entorno digital interconectado.
- La ciberseguridad es esencial para proteger activos críticos.
- El hacking ético se presenta como una defensa proactiva.



## ¿Qué es la Ciberseguridad?

Protección de sistemas, redes y datos.

Objetivo: asegurar **confidencialidad, integridad y disponibilidad**.

Áreas clave:

- Seguridad de la información y aplicaciones
- Seguridad de redes
- Gestión de accesos e incidentes



## ⚠ Amenazas Cibernéticas

### Internas:

- Empleados con privilegios mal usados

### Externas:

- Actores maliciosos que explotan vulnerabilidades

### Principales amenazas:

- Malware (virus, ransomware)
- Phishing (engaño por identidad)
- Ataques de red (DDoS, spoofing, MITM)






## Vulnerabilidades Comunes

- Inyección SQL
- Cross-Site Scripting (XSS)
- Gestión insegura de sesiones
- Exposición de datos sensibles



## ¿Quiénes son los ciberatacantes?

- **Black Hat:** dañinos, buscan lucro o destrucción
- **White Hat:** hackers éticos, trabajan para proteger
- **Grey Hat:** sin permiso, pero no necesariamente maliciosos

 El **hacking ético** aplica las mismas técnicas de los atacantes, pero para defender.



## 💥 Impactos si no actuamos

- **Financieros:** pagos, pérdidas operativas
- **Reputacionales:** pérdida de confianza
- **Legales:** sanciones por normativas (ej. GDPR, LGPD)
- **Operativos:** paralización de servicios

### Casos reales:

- WannaCry, Colonial Pipeline, Log4Shell



## Ciberguerra y Ciberdefensa Avanzada

- Uso de ataques para propósitos políticos y militares
- Modelos como **Cyber Kill Chain** ayudan a:
  - i. Detectar
  - ii. Entender
  - iii. Mitigar
  - iv. Responder a amenazas avanzadas





## Conclusión

- La ciberseguridad no es solo técnica, es estratégica.
- El conocimiento profundo es la mejor defensa.
- El pensamiento ofensivo se convierte en **protección activa**.



