# CyberSentinel-AI Academy: Guia Visual

## Capitulo 1: Fundamentos (Escenario Banco)

*[ESPACIO PARA DIAGRAMA: Modelo STRIDE]*

### Flujo de Ataque (Rojo):

1. Spoofing: Falsificacion de identidad.
2. Tampering: Modificacion de datos.
3. Elevation: Escalada de privilegios.

### Defensa (Azul):

- MFA (Autenticacion Multifactor).
- Firmas digitales y Hashing.

*Ver modulo completo: /Capitulo_1*

## Capitulo 2: Arquitectura Segura

*[ESPACIO PARA DIAGRAMA: El Bastion Digital (Firewall)]*

### Flujo Normal (Verde):

Usuario -> Puerto 443 (HTTPS) -> Servidor Web.

### Flujo Bloqueado (Rojo/Azul):

Atacante -> Puerto 22 (SSH) -> [X] Firewall (DROP).

*Ver modulo completo: /Capitulo_2*

# CyberSentinel-AI Academy: Guia Visual

## Capitulo 3: Seguridad Moderna con IA

*[ESPACIO PARA DIAGRAMA: Deteccion ML vs Reglas]*

### Flujo de Deteccion Moderna:

1. Logs entrantes: Datos crudos.
2. Reglas: Alerta Rapida.
3. ML: Analisis Profundo de Comportamiento.

### Ventajas:

- Detecta 0-days (desconocidos).
- Reduce falsos positivos.

*Ver modulo completo: /Capitulo_3*

## Capitulo 4: IA Ofensiva

*[ESPACIO PARA DIAGRAMA: Ciclo de Ataque con LLMs]*

### Ciclo:

1. Prompt -> 2. Generacion -> 3. Validacion Humana -> 4. Ejecucion Controlada

*Ver modulo completo: /Capitulo_4*

# CyberSentinel-AI Academy: Guia Visual

## Capitulo 5: Operaciones (SCADA)

*[ESPACIO PARA DIAGRAMA: Defensa de Infraestructura Critica]*

**Zonas:**

IT (Oficina) -> DMZ -> OT (Planta Aislada)

**Defensa (Azul):**

- Diodo de Datos (Solo salida).
- IPS Industrial.

*Ver modulo completo: /Capitulo_5*

## Capitulo 6: Respuesta a Incidentes

*[ESPACIO PARA DIAGRAMA: Ciclo NIST]*

**Fases:**

Preparacion -> Deteccion -> Contencion -> Erradicacion -> Recuperacion

*Ver modulo completo: /Capitulo_6*