

# Seguridad Física y Controles de Acceso

DEFINICIONES, FUNCIONAMIENTO Y CUIDADOS

FRANCISCO OCHOA ORNELAS – 2025

# Índice



1. Riesgos físicos relevantes



2. Medidas de seguridad física y funcionamiento



3. Acceso no autorizado, políticas y modelos de seguridad



4. Conclusión

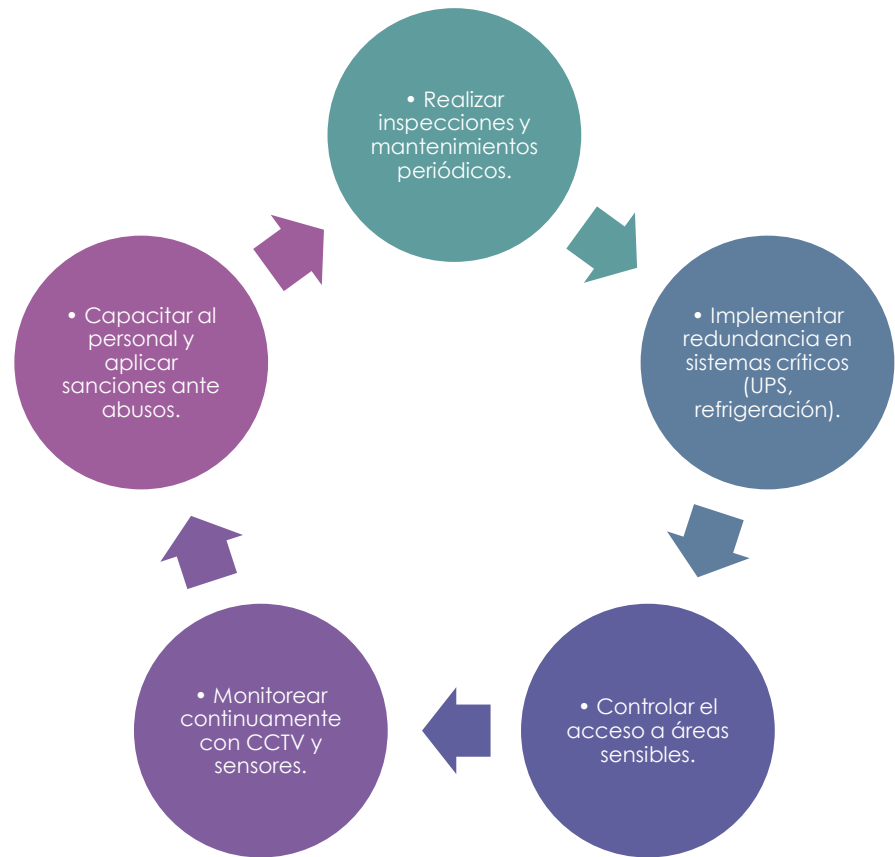


5. Referencias

# Riesgos Físicos Relevantes

- Daño: deterioro o destrucción de bienes físicos por accidente o negligencia.
- Robo/Hurto: sustracción de bienes, con o sin uso de fuerza.
- Sabotaje: daño deliberado a instalaciones o sistemas.
- Espionaje: extracción de información confidencial.
- Mal uso/Abuso: empleo indebido de recursos físicos o tecnológicos.

# Funcionamiento y Cuidados



# Perímetro y Control de Acceso

1

- Perímetro: primera barrera de seguridad, con vallas, muros y sensores.

2

- Control de acceso: tarjetas, biometría y gestión de visitantes.

3

- Cuidados: mantener iluminación adecuada y auditorías periódicas de accesos.

# Alarmas, Sensores y CCTV

- Alarmas detectan intrusiones mediante sensores de movimiento o vibración.



- CCTV monitorea áreas críticas en tiempo real.



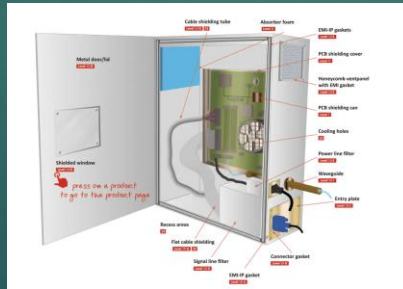
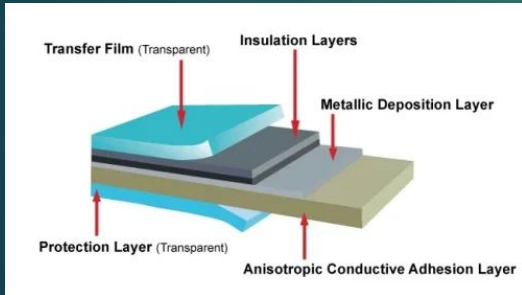
- Cuidados: limpieza de lentes, calibración de sensores, respaldo energético.

# UPS, Piso Elevado y Aire Acondicionado

- ▶ • UPS: evita pérdida de energía y protege equipos.
- ▶ • Piso elevado: facilita cableado y ventilación controlada.
- ▶ • Aire acondicionado: mantiene condiciones térmicas estables.
- ▶ • Cuidados: mantenimiento preventivo, limpieza y pruebas de respaldo.

# Escudos RF y EM

- ▶ • Bloquean o atenúan señales electromagnéticas (salas Faraday, blindajes).
- ▶ • Funcionamiento: reflejan o absorben ondas electromagnéticas.
- ▶ • Cuidados: verificar continuidad del blindaje, evitar filtraciones por cables.





# Acceso No Autorizado y Políticas

- ▶ • Acceso no autorizado: uso o ingreso sin permiso.
- ▶ • Políticas de seguridad: establecen reglas para la protección de activos.
- ▶ • Modelos: RBAC (roles), ABAC (atributos), DAC (discrecional), MAC (mandatorio).

# Conclusión

- ▶ • La seguridad física complementa la cibernética.
- ▶ • La prevención es más eficaz que la respuesta al incidente.
- ▶ • La formación del personal es clave para evitar sabotajes o abusos.
- ▶ • Auditorías regulares garantizan funcionamiento óptimo de controles físicos.



# Referencias

- ▶ • CISA. Physical Security Best Practices, 2024.
- ▶ • Center for Internet Security (CIS). Physical Security Controls, 2023.
- ▶ • NIST SP 800-53. Security and Privacy Controls, 2023.
- ▶ • Microsoft Docs. What is Access Control, 2024.
- ▶ • ISACA. Physical and Environmental Security Guidelines, 2022.