

Unidad 2

Seguridad Física

Apunte de Cátedra · Seguridad y Auditoría Informática

Contenidos de la Unidad 2

01

Concepto de Seguridad Física

Qué es, qué protege y por qué es fundamental

02

Protección de Instalaciones

Medidas generales y ubicación de edificios

03

Áreas Seguras y Perímetros

Zonificación y barreras físicas

04

Control de Acceso Físico

Proceso, mecanismos, CCTV y alarmas

05

Protección contra Incendios

Triángulo/tetraedro, clases y extintores

06

Protección Eléctrica y Ambiental

UPS, generadores, riesgos ambientales

07

Centros de Datos

Componentes y medidas de seguridad física

2.1 Introducción

La Seguridad Física es la primera línea de defensa

Más que software

Antivirus, firewalls y MFA pierden efectividad si cualquiera puede entrar a la sala de servidores y desconectar o sustraer equipos.

Amenazas físicas

Accesos no autorizados, robos, incendios, inundaciones, fallas eléctricas, condiciones ambientales y sabotaje.

Protección integral

Políticas, procedimientos, tecnologías y controles para proteger personas, instalaciones, equipos y soportes físicos.

Primera línea

Antes de proteger los datos con mecanismos lógicos, hay que proteger el lugar donde se almacenan y procesan.

2.2 ¿Qué es la Seguridad Física?

Conjunto de políticas, procedimientos, controles y medidas destinadas a proteger las personas, las instalaciones, los equipos y los soportes físicos de información frente a amenazas de origen físico, ya sean accidentales o intencionales.

Seguridad Física vs Seguridad Lógica

Seguridad Física

Protege el entorno material: edificios, salas, equipos, cableado, documentación en papel.

Seguridad Lógica

Protege mediante software: autenticación, cifrado, firewalls, control de acceso lógico.

2.2.3 Importancia de la Seguridad Física

Basta un único incidente físico para inutilizar todos los mecanismos de seguridad lógica implementados.

Incendio

Destruye el centro de cómputos. Si los backups estaban en el mismo edificio → pérdida irreversible.

Acceso físico

Un atacante entra a la sala de servidores, apaga equipos, sustrae discos o instala hardware malicioso.

Falla eléctrica

Corte prolongado sin UPS ni generador → interrupción total de operaciones y posible corrupción de datos.

2.2.4 ¿Qué protege la Seguridad Física?

Edificios e instalaciones

Oficinas, centros de cómputos, salas técnicas

Equipos informáticos

Servidores, PCs, dispositivos de almacenamiento

Equipos de red

Routers, switches, cableado estructurado

Sistemas de soporte

Eléctricos, climatización, detección de incendios

Documentación física

Papeles, soportes, archivos confidenciales

Personas

Integridad física de quienes trabajan en la organización

2.2.5 Principios fundamentales

1

Protección por capas

Múltiples barreras sucesivas. Ejemplo: tarjeta → credencial → biometría → registro → CCTV.

2

Defensa en profundidad

Ningún control es suficiente solo. Si uno falla, los demás siguen protegiendo.

3

Disponibilidad

Garantizar que los sistemas permanezcan operativos el mayor tiempo posible.

4

Continuidad operativa

Preparar la organización para seguir funcionando cuando ocurre un incidente (redundancia, generadores, etc.).

2.2.6 Amenazas de origen físico

Amenazas naturales

- Terremotos
- Inundaciones
- Tormentas
- Incendios forestales
- Altas temperaturas
- Descargas atmosféricas

No se pueden evitar, pero sí reducir su impacto con planificación.

Amenazas humanas

- Robo de equipos
- Vandalismo y sabotaje
- Accesos no autorizados
- Manipulación incorrecta
- Incendios por negligencia
- Cortes intencionales de energía

Pueden ser accidentales o intencionales.

2.3 Protección de Instalaciones

Las instalaciones son el primer nivel de protección física.

Conjunto de medidas físicas, organizativas y técnicas destinadas a proteger edificios, oficinas, salas técnicas y espacios donde se desarrollan las actividades, evitando daños por amenazas naturales o humanas.

Ubicación

Riesgo sísmico, inundaciones, proximidad a riesgos industriales

Conservación

Mantenimiento de techos, puertas, instalaciones eléctricas

Iluminación

Seguridad de personas + efecto disuasorio nocturno

Señalización

Salidas de emergencia, rutas, extintores, zonas restringidas

Orden y limpieza

Evitar obstáculos, materiales inflamables y objetos extraños

Mantenimiento

Inspección periódica antes de que ocurran fallas

2.4 Áreas Seguras

Espacio físico al que únicamente pueden acceder personas autorizadas, porque contiene activos cuya pérdida, alteración o destrucción produciría un impacto significativo.

Ejemplos de áreas seguras

Centros de cómputos

Salas de servidores

Salas de comunicaciones

Archivos confidenciales

Salas de backups

Laboratorios de investigación

Clasificación de áreas según nivel de acceso

Público

Acceso libre

Recepción, sala de espera

Interno

Solo empleados

Oficinas administrativas

Restringido

Personal autorizado

Área de informática

Crítico

Altamente controlado

Centro de Datos (cómpu

2.4.3 Perímetros de Seguridad

Límite físico que delimita un área protegida e implementa controles para detectar, retrasar o impedir el ingreso de personas no autorizadas.

Funciones principales



Delimitar

Identificar dónde comienza la zona restringida



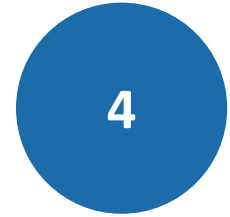
Disuadir

Barreras visibles reducen intentos de intrusión



Retrasar

Ganar tiempo para detección y respuesta



Detectar

Sensores, CCTV y alarmas asociados al perímetro

2.5 Control de Acceso Físico

Conjunto de medidas que permiten identificar, autenticar y autorizar a las personas que intentan ingresar a una instalación o área restringida, registrando el acceso cuando corresponde.

Objetivos

1. Impedir el acceso de personas no autorizadas
2. Permitir el ingreso solo a personal autorizado
3. Registrar quién entra y sale (trazabilidad)
4. Detectar intentos de acceso indebido
5. Aplicar el principio de mínimo privilegio

2.5.4 El proceso de control de acceso

1

Identificación

La persona se identifica (credencial, documento, biometría)

2

Autenticación

Se verifica que es quien dice ser (PIN, huella, tarjeta)

3

Autorización

Se comprueba si tiene permiso para ese recurso o zona

4

Registro

Se registra el evento (quién, cuándo, dónde, resultado)

2.5.5 Principio de mínimo privilegio

Cada persona debe tener únicamente el acceso físico estrictamente necesario para cumplir sus funciones. Ni más ni menos.

Empleado administrativo

Acceso a oficinas y áreas comunes. No al centro de datos.

Técnico de sistemas

Acceso a salas de servidores según su rol y horario.

Visitante

Solo zonas públicas, acompañado y registrado.

Personal de limpieza

Acceso controlado, fuera de horarios críticos, con supervisión.

2.5.6 Mecanismos de Control de Acceso

Factor 1

Algo que se posee

Tarjeta, llave, token, celular

Factor 2

Algo que se conoce

PIN, contraseña, código

Factor 3

Algo que se es

Huella, iris, rostro, voz

Ejemplos de implementación

- Tarjetas de proximidad (RFID/NFC) · Códigos PIN · Biometría (huella, facial)
- Torniquetes y esclusas · Cerraduras electrónicas · Control de visitantes
- Autenticación multifactor física (tarjeta + PIN o biometría)

2.5.6 Mecanismos de Control de Acceso - Biometría

Sistemas biométricos

Un sistema biométrico es un mecanismo de autenticación que verifica la identidad de una persona mediante el análisis de características físicas o comportamentales que resultan difíciles de falsificar.



Oreja



Geometría de la mano



Estructura venosa



Retina



Termografía facial



Huella Dactilar



Iris



Voz



Firma



Cara

Tecnología	Precisión	Costo	Facilidad de uso	Uso habitual
Huella digital	Alta	Bajo	Muy alta	Empresas, universidades
Reconocimiento facial	Alta	Medio	Muy alta	Edificios inteligentes
Iris	Muy alta	Alto	Alta	Infraestructura crítica
Geometría de mano	Media	Medio	Alta	Industria
Voz	Media	Bajo	Alta	Call Centers

2.5.6 Mecanismos de Control de Acceso - Biometría

Rasgos Biométricos mas utilizados:

Huellas dactilares: El uso de las huellas dactilares como medio de identificación es de alta fiabilidad. Tiene buena aceptación y popularidad.



Ojo: La identificación de un individuo a través del análisis del iris tiene una fiabilidad muy alta. El problema es la facilidad de uso. El análisis de la retina para identificar al individuo es más complejo todavía.



2.5.6 Mecanismos de Control de Acceso - Biometría

Rasgos Biométricos mas utilizados:

Forma de la mano: Este sistema está bastante extendido, pero quizás presenta un poco menos de fiabilidad que los anteriores. Este sistema es susceptible de padecer ataques, puesto que no resultaría difícil recrear la forma de una mano usando un molde.



Venas del dedo o la mano: El estudio vascular de los dedos o de la mano proporciona alta fiabilidad, además no es muy complejo su análisis.



2.5.9 CCTV y Sistemas de Alarmas

Videovigilancia (CCTV)

Funciones:

- Disuasión
- Detección de incidentes
- Evidencia posterior
- Monitoreo en tiempo real

Ubicaciones típicas:

- Accesos y perímetros
- Salas de servidores
- Estacionamientos
- Áreas de almacenamiento

Sistemas de Alarmas

De intrusión:

- Sensores de apertura
- Sensores de movimiento
- Barreras infrarrojas
- Detectores de vibración

Contra incendios:

- Detectores de humo
- Detectores de temperatura
- Detectores de llama
- Alarmas sonoras y visuales

2.6 Protección contra Incendios

No se limita a disponer de extintores. Combina prevención, detección, extinción y evacuación.

Prevención

Eliminar causas que originan incendios

Diseño seguro

Materiales, compartimentación, rutas

Detección temprana

Detectores de humo, temperatura, llama

Extinción

Automática y manual (extintores)

Evacuación

Planes, señalización, puntos de reunión

Capacitación

Personal entrenado en respuesta

2.6.4 – 2.6.5 Triángulo y Tetraedro del Fuego

Triángulo del Fuego

Tres elementos necesarios:

1. Combustible
(papel, plástico, cableado...)
2. Comburente
(oxígeno del aire)
3. Calor
(cortocircuito, chispa...)

Eliminar cualquiera interrumpe la combustión.

Tetraedro del Fuego

Agrega un 4º elemento:

4. Reacción química en cadena
(radicales libres que mantienen la combustión)

Explica por qué ciertos agentes (polvo químico seco) interrumpen la reacción.

Métodos de extinción:

- Retirar combustible
- Reducir oxígeno
- Bajar temperatura
- Interrumpir la reacción

2.6.6 Clasificación de los incendios

Clase A

Sólidos

Madera, papel, telas, muebles

Clase B

Líquidos / gases

Nafta, alcohol, solventes, GLP

Clase C

Equipos eléctricos

Servidores, UPS, tableros, cableado

Clase D

Metales combustibles

Magnesio, sodio, titanio, litio

Clase K

Aceites y grasas

Cocinas industriales

2.6.7 Extintores según tipo de incendio

Clase	Tipo de fuego	Extintores recomendados
A	Sólidos combustibles	Agua · Espuma · Polvo ABC
B	Líquidos inflamables	Espuma · CO ₂ · Polvo ABC
C	Equipos eléctricos	CO ₂ · Polvo ABC · Agentes limpios
D	Metales combustibles	Polvo especial clase D
K	Aceites y grasas	Agentes químicos húmedos

Nunca usar agua en fuegos clase B o C. Puede agravar la situación o causar electrocución.

2.7 Protección Eléctrica

Garantizar un suministro seguro y confiable para personas y equipos.

Corte de energía

Interrupción, pérdida de datos,
apagado inesperado

Sobretensión

Daños en componentes electrónicos
sensibles

Subtensión

Reinicios y funcionamiento inestable

Sobrecarga

Sobrecalentamiento y riesgo de
incendio

Cortocircuito

Corriente elevada, daños e
incendios

Descargas atmosféricas

Sobretensiones por rayos

Dispositivos de protección eléctrica

Puesta a tierra

Deriva corrientes de falla. Protege personas y equipos.

Llave térmica

Protege contra sobrecargas y cortocircuitos (instalación).

Disyuntor diferencial

Detecta fugas a tierra. Protege principalmente a las personas.

Protector sobretensiones

Limita picos de tensión que dañan equipos electrónicos.

2.7.6 Sistemas de Alimentación de Respaldo

UPS

- Energía inmediata desde baterías
- Transición casi instantánea
- Autonomía limitada (minutos)
- Protege servidores, switches, almacenamiento
- Tiempo para apagar o esperar generador

Generador eléctrico

- Arranque en segundos
- Alimentación prolongada
- Combustible (diésel, gas, nafta)
- Hospitales, data centers, bancos
- Requiere mantenimiento regular

La UPS cubre los primeros segundos/minutos. El generador mantiene el suministro en cortes prolongados. Son complementarios.

2.7.8 Cuadro resumen de dispositivos

Dispositivo	¿Qué detecta / hace?	¿Qué protege?
Puesta a tierra	Deriva corrientes de falla	Personas y equipos
Llave térmica	Sobrecarga y cortocircuito	Instalación y equipos
Disyuntor diferencial	Corriente de fuga a tierra	Personas
Protector sobretensiones	Aumento de tensión	Equipos electrónicos
UPS	Corte de energía (inmediato)	Continuidad del servicio
Generador eléctrico	Corte prolongado	Continuidad operativa

2.8 Protección Ambiental

Controlar las condiciones del entorno donde funcionan los equipos informáticos.

Temperatura elevada

Reduce rendimiento, acelera desgaste, puede causar apagados automáticos.

Humedad

Excesiva → corrosión y cortocircuitos. Muy baja → electricidad estática.

Polvo

Obstruye ventilación, favorece sobrecalentamiento y reduce vida útil.

Agua / inundaciones

Daño físico, cortocircuitos y pérdida de información.

Vibraciones

Afectan discos y equipos delicados, especialmente en entornos industriales.

2.9 Centros de Datos

Instalación diseñada para alojar y proteger la infraestructura tecnológica: servidores, almacenamiento, redes y sistemas de soporte, con condiciones ambientales y de seguridad controladas.

Componentes principales

Servidores

Almacenamiento

Equipos de red

Racks

Cableado estructurado

Alimentación eléctrica

Climatización

Detección/extinción de incendios

Control de acceso y CCTV

2.9.3 Medidas de Seguridad Física en un Centro de Datos

Control de acceso

Tarjetas, biometría, MFA, registros de ingreso

Videovigilancia

Monitoreo interior y exterior, evidencias

Protección incendios

Detectores, agentes limpios, extintores CO₂

Protección eléctrica

Puesta a tierra, UPS, generadores, protectores

Control ambiental

Temperatura, humedad, polvo, sensores de agua

Redundancia

Alimentación, climatización y enlaces duplicados

Integración de la Seguridad Física

Todos los controles se complementan para proteger la infraestructura

- | | | |
|---|-------------------------------|---|
| 1 | Instalaciones | Ubicación, mantenimiento, iluminación, señalización |
| 2 | Áreas y perímetros | Zonificación y barreras físicas |
| 3 | Control de acceso | Identificación, autenticación, autorización, CCTV, alarmas |
| 4 | Incendios y eléctrica | Detección, extinción, UPS, generadores, puesta a tierra |
| 5 | Ambiente y Data Center | Climatización, sensores y medidas específicas del centro de datos |

Unidad 2 completada

Seguridad Física

¿Preguntas?

Facultad de Ingeniería · Universidad Nacional de Jujuy