Facultad de Ingeniería

Unidad 2. Seguridad Física

Apunte de cátedra

Contenido

2. Seguridad física 4

2.1. Introducción 4

2.1.1. Relación entre los temas de la unidad 5

2.2. Concepto de Seguridad Física 5

2.2.1. Introducción 5

2.2.2. ¿Qué es la Seguridad Física? 6

2.2.3. La importancia de la Seguridad Física 6

2.2.4. ¿Qué protege la Seguridad Física? 7

2.2.5. Principios fundamentales de la Seguridad Física 7

2.2.6. Las amenazas de origen físico 9

2.3. Protección de Instalaciones 9

2.3.1. Introducción 9

2.3.2. Concepto de protección de instalaciones 10

2.3.3. Importancia de la protección de instalaciones 10

2.3.4. Medidas generales para la protección de instalaciones 11

2.3.5. Ejemplo de aplicación 13

2.4. Áreas Seguras y Perímetros de Seguridad 14

2.4.1. Introducción 14

2.4.2. Concepto de Áreas Seguras 14

2.4.3. Concepto de Perímetro de Seguridad 16

2.4.4. Relación entre Áreas Seguras y Perímetros de Seguridad 17

2.4.5. Ejemplo de aplicación 18

2.5. Control de Acceso Físico 18

2.5.1. Introducción 18
2.5.2. Concepto de Control de Acceso Físico 19
2.5.3. Objetivos del Control de Acceso 19
2.5.4. El proceso de control de acceso 19
2.5.5. El principio de mínimo privilegio aplicado al acceso físico 21
2.5.6. Mecanismos de Control de Acceso 21
2.5.7. Ejemplo de aplicación 27
2.5.8. Relación del Control de Acceso con otros apartados de la unidad 28
2.5.9. Sistemas de Videovigilancia (CCTV) y Sistemas de Alarmas 28
2.5.10. Sistemas de Alarmas 31
2.6. Protección contra Incendios 36
2.6.1. Concepto 36
2.6.2. Concepto de fuego 36
2.6.3. Concepto de incendio 37
2.6.4. El Triángulo del Fuego 37
2.6.5. El Tetraedro del Fuego 38
2.6.6. Clasificación de los incendios 39
2.6.7. Extintores según tipo de incendios 41
2.7. Protección Eléctrica 42
2.7.1. Concepto y objetivos 42
2.7.2. Objetivos de la protección eléctrica 43
2.7.3. Riesgos eléctricos 43
2.7.4. Puesta a tierra 43
2.7.5. Interruptores automáticos 44

2.7.6. Sistemas de Alimentación de Respaldo 46
2.7.7. Relación entre la UPS y el generador eléctrico 47
2.7.8. Cuadro resumen de los dispositivos estudiados 48
2.8. Protección Ambiental 48
2.8.1. Concepto 48
2.8.2. Principales riesgos ambientales 48
2.9. Centros de Datos 49
2.9.1. Concepto 49
2.9.2. Componentes principales de un Centro de Datos 49
2.9.3. Medidas de Seguridad Física en un Centro de Datos 51

2. Seguridad física
2.1. Introducción

Cuando se habla de seguridad informática es frecuente pensar únicamente en antivirus, firewalls, autenticación multifactor o cifrado de la información. Sin embargo, todos estos mecanismos pueden resultar insuficientes si la infraestructura física donde se encuentran los equipos informáticos no dispone de medidas de protección adecuadas.

Un servidor puede contar con los sistemas de seguridad lógica más avanzados del mercado, pero si cualquier persona puede ingresar a la sala donde se encuentra instalado y desconectarlo, sustraer sus discos o destruirlo físicamente, toda la estrategia de seguridad pierde efectividad. De la misma manera, una organización puede invertir grandes recursos en proteger su red informática, pero un incendio, una inundación o una falla eléctrica prolongada pueden ocasionar la interrupción total de sus operaciones.

La Seguridad Física constituye, por lo tanto, uno de los pilares fundamentales de la Seguridad de la Información. Su propósito es proteger las personas, las instalaciones, los equipos y los medios físicos donde se almacena, procesa o transmite la información frente a amenazas de origen físico, tanto accidentales como intencionales.

Estas amenazas pueden provenir de múltiples fuentes, entre ellas:

- accesos físicos no autorizados;
- robos o vandalismo;
- incendios;
- inundaciones;
- terremotos;
- fallas eléctricas;
- condiciones ambientales inadecuadas;
- errores humanos;
- actos de sabotaje.

La implementación de controles físicos adecuados reduce considerablemente la probabilidad de que estas amenazas produzcan incidentes capaces de afectar la confidencialidad, integridad o disponibilidad de la información.

En las organizaciones modernas, la Seguridad Física no se limita únicamente a colocar cerraduras o instalar cámaras de vigilancia. Comprende un conjunto de políticas, procedimientos, tecnologías y controles destinados a proteger toda la infraestructura que soporta los sistemas de información. Esto incluye el diseño de edificios, la definición de áreas restringidas, el control del acceso de personas, la protección contra incendios, la disponibilidad del suministro eléctrico, el monitoreo ambiental y la implementación de centros de datos especialmente diseñados para garantizar la continuidad de las operaciones.

En consecuencia, puede afirmarse que la Seguridad Física constituye la primera línea de defensa de una organización. Antes de proteger los datos mediante mecanismos lógicos,

resulta imprescindible proteger físicamente el lugar donde esos datos se encuentran almacenados y procesados.

2.1.1. Relación entre los temas de la unidad

Uno de los errores más frecuentes consiste en considerar que los distintos temas de la Seguridad Física son independientes entre sí. En realidad, todos ellos responden a un objetivo común: **proteger físicamente la infraestructura que soporta los sistemas de información**.

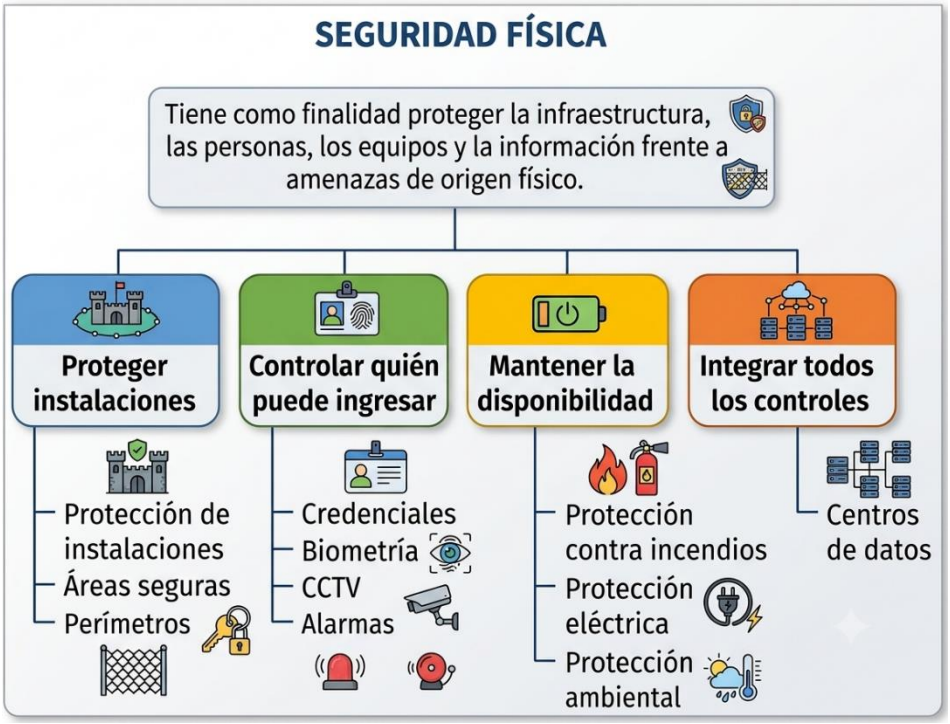

Figura 2.1. Relación de los contenidos de la unidad

Este esquema será utilizado como guía durante toda la unidad. Cada apartado estudiará uno de estos grupos de controles y, al finalizar, el estudiante podrá comprender cómo todos ellos se integran para proteger la infraestructura física de una organización.

2.2. Concepto de Seguridad Física

2.2.1. Introducción

La información constituye uno de los activos más valiosos de cualquier organización. Sin embargo, dicha información no existe de manera aislada: se almacena en servidores, computadoras, dispositivos de almacenamiento, documentos impresos y otros medios físicos que requieren un entorno adecuado para garantizar su funcionamiento.

Cuando se analizan los incidentes de seguridad informática, es frecuente asociarlos con ataques realizados a través de Internet, malware, vulnerabilidades de software o accesos indebidos a sistemas informáticos. Aunque estas amenazas representan un riesgo

importante, existen numerosos incidentes cuyo origen no se encuentra en el ámbito lógico, sino en el entorno físico donde operan los sistemas de información.

Por ejemplo, una inundación puede destruir el centro de datos de una empresa; un incendio puede dejar fuera de servicio los servidores corporativos; una falla prolongada del suministro eléctrico puede provocar la pérdida de información; o una persona sin autorización puede ingresar a una sala de servidores y sustraer un equipo crítico. En todos estos casos, la confidencialidad, integridad y disponibilidad de la información se ven comprometidas, aun cuando los sistemas informáticos cuenten con mecanismos avanzados de seguridad lógica.

Por esta razón, la protección física constituye uno de los pilares fundamentales de cualquier estrategia de seguridad informática. Antes de proteger la información mediante mecanismos tecnológicos, resulta indispensable proteger el lugar donde dicha información se almacena, procesa y transmite.

2.2.2. ¿Qué es la Seguridad Física?

La **Seguridad Física** es el 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.

Su finalidad principal es preservar la continuidad de las operaciones de la organización evitando que eventos físicos provoquen daños sobre los activos de información.

A diferencia de la **Seguridad Lógica**, cuyo objetivo es impedir accesos indebidos a los sistemas mediante controles de software, autenticación, cifrado o firewalls, la Seguridad Física protege el entorno material donde funcionan dichos sistemas.

En consecuencia, ambas disciplinas no compiten entre sí, sino que se complementan para proporcionar una protección integral de la información.

2.2.3. La importancia de la Seguridad Física

En muchas organizaciones existe la falsa percepción de que la seguridad informática depende exclusivamente del software. Esta idea conduce a invertir importantes recursos en antivirus, firewalls o sistemas de detección de intrusiones, mientras se descuidan aspectos tan importantes como el control de acceso a las instalaciones, la protección eléctrica o la prevención de incendios.

Sin embargo, basta un único incidente físico para inutilizar todos los mecanismos de seguridad lógica implementados.

Supongamos que una empresa dispone de:

- autenticación multifactor;
- cifrado de bases de datos;

- firewall de última generación;
- sistema de detección de intrusiones;
- copias de seguridad diarias.

Si un incendio destruye el centro de cómputos y las copias de seguridad se almacenaban en el mismo edificio, toda la información puede perderse de forma irreversible.

Del mismo modo, si un atacante consigue ingresar físicamente a la sala de servidores, podría apagar los equipos, sustraer discos duros o instalar dispositivos maliciosos sin necesidad de vulnerar ninguna contraseña.

Estos ejemplos demuestran que la seguridad lógica pierde efectividad cuando no está acompañada por adecuados controles físicos.

2.2.4. ¿Qué protege la Seguridad Física?

La Seguridad Física protege todos aquellos activos materiales que intervienen en el funcionamiento de los sistemas de información.

Entre ellos se encuentran:

- edificios e instalaciones;
- centros de cómputos;
- salas de comunicaciones;
- servidores;
- computadoras personales;
- dispositivos de almacenamiento;
- equipos de red;
- cableado;
- sistemas eléctricos;
- sistemas de climatización;
- documentación en papel;
- soportes físicos de información.

No todos estos activos poseen el mismo nivel de criticidad. Por ejemplo, la pérdida de una computadora utilizada para tareas administrativas puede ocasionar inconvenientes limitados, mientras que un daño en el servidor principal de una organización puede interrumpir completamente sus operaciones.

Por este motivo, uno de los principios fundamentales de la Seguridad Física consiste en identificar cuáles son los activos críticos y establecer medidas de protección acordes con su importancia.

2.2.5. Principios fundamentales de la Seguridad Física

Aunque las organizaciones pueden implementar diferentes controles físicos según su tamaño y actividad, existen algunos principios generales que orientan el diseño de cualquier sistema de protección.

2.2.5.1. Protección por capas

La Seguridad Física no debe depender de un único mecanismo de protección. En lugar de instalar solamente una puerta con cerradura, resulta más efectivo implementar múltiples barreras sucesivas, de manera que un atacante deba superar varios niveles de protección para acceder a un activo crítico.

Por ejemplo, el acceso a un centro de cómputos podría requerir:

- ingreso al edificio mediante tarjeta magnética;
- acceso al sector de informática mediante credencial;
- autenticación biométrica para ingresar a la sala de servidores;
- registro automático del ingreso;
- videovigilancia permanente.

Cada una de estas medidas incrementa el nivel de seguridad y reduce la probabilidad de un acceso no autorizado.

2.2.5.2. Defensa en profundidad

El principio de defensa en profundidad establece que ningún control de seguridad debe considerarse suficiente por sí solo.

Si un mecanismo falla, los restantes controles deben continuar proporcionando protección.

Por ejemplo, una cámara de videovigilancia no impide físicamente el ingreso de una persona; únicamente registra lo ocurrido. Por ello debe complementarse con puertas de seguridad, sistemas de autenticación, alarmas y procedimientos de vigilancia.

2.2.5.3. Disponibilidad

Uno de los objetivos fundamentales de la Seguridad Física consiste en garantizar que los sistemas permanezcan operativos el mayor tiempo posible.

Para ello resulta necesario proteger la infraestructura frente a incendios, cortes de energía, inundaciones y otras amenazas capaces de interrumpir el funcionamiento normal de la organización.

2.2.5.4. Continuidad operativa

No basta con prevenir incidentes; también es necesario preparar a la organización para continuar funcionando cuando un incidente ocurre.

Por ello se implementan sistemas redundantes, fuentes alternativas de energía, generadores eléctricos y centros de cómputos diseñados para mantener los servicios esenciales aun durante situaciones de emergencia.

2.2.6. Las amenazas de origen físico

Las amenazas físicas pueden clasificarse, de manera general, en dos grandes grupos.

2.2.6.1. Amenazas naturales

Son aquellas originadas por fenómenos de la naturaleza y que escapan al control de la organización.

Entre ellas pueden mencionarse:

- terremotos;
- inundaciones;
- tormentas;
- incendios forestales;
- altas temperaturas;
- descargas eléctricas atmosféricas.

Estas amenazas no pueden evitarse, pero sí es posible reducir su impacto mediante una adecuada planificación de la infraestructura.

2.2.6.2. Amenazas provocadas por el ser humano

Pueden ser accidentales o intencionales.

Algunos ejemplos son:

- robo de equipos;
- vandalismo;
- sabotaje;
- accesos físicos no autorizados;
- manipulación incorrecta de equipos;
- incendios ocasionados por negligencia;
- cortes intencionales del suministro eléctrico.

2.3. Protección de Instalaciones

2.3.1. Introducción

Las instalaciones representan el primer nivel de protección física. Constituyen el entorno donde se encuentran las personas, los equipos informáticos, las redes de comunicación y los soportes de información. Por esta razón, un diseño inadecuado de las instalaciones

puede incrementar considerablemente la probabilidad de que ocurra un incidente de seguridad.

La protección de instalaciones comprende el conjunto de medidas destinadas a reducir el riesgo de daños ocasionados por amenazas externas e internas, garantizando que los edificios y las áreas de trabajo proporcionen un entorno seguro para el funcionamiento de los sistemas de información.

No todas las organizaciones requieren el mismo nivel de protección. Un pequeño estudio profesional presenta necesidades diferentes a las de un banco, un hospital o un centro de cómputos. Sin embargo, existen principios generales que pueden aplicarse a cualquier organización.

2.3.2. Concepto de protección de instalaciones

La **protección de instalaciones** consiste en el conjunto de medidas físicas, organizativas y técnicas destinadas a proteger los edificios, oficinas, salas técnicas y demás espacios donde se desarrollan las actividades de una organización, evitando daños ocasionados por amenazas naturales o provocadas por el ser humano.

Su finalidad no es únicamente impedir el ingreso de personas no autorizadas, sino también minimizar los efectos de eventos que puedan afectar la infraestructura física, tales como incendios, inundaciones, actos de vandalismo o accidentes.

En otras palabras, mientras la Seguridad Física constituye el marco general de protección, la protección de instalaciones se enfoca específicamente en el edificio y en los espacios físicos donde se encuentran los activos de la organización.

2.3.3. Importancia de la protección de instalaciones

Las instalaciones representan el primer nivel de defensa frente a numerosas amenazas.

Un edificio correctamente diseñado puede dificultar el acceso de personas no autorizadas, reducir los efectos de un incendio, minimizar el impacto de fenómenos climáticos y facilitar la evacuación de las personas en caso de emergencia.

Por el contrario, instalaciones mal diseñadas o deficientemente mantenidas incrementan la probabilidad de incidentes y pueden comprometer la continuidad operativa de la organización.

La ubicación de los equipos críticos también influye en el nivel de seguridad. Por ejemplo, instalar servidores en oficinas de acceso público o almacenar documentación confidencial en lugares sin restricciones facilita el acceso indebido y aumenta el riesgo de pérdida o manipulación de la información.

En consecuencia, la protección de instalaciones constituye la base sobre la cual se implementarán posteriormente otros controles, como las áreas seguras, los perímetros de seguridad y el control de acceso físico.

2.3.4. Medidas generales para la protección de instalaciones

La protección de instalaciones no depende de una única medida de seguridad, sino de la aplicación coordinada de diversos controles físicos, administrativos y organizativos. El objetivo es reducir la probabilidad de que una amenaza pueda afectar el funcionamiento normal de la organización.

Entre las medidas más utilizadas se encuentran las siguientes.

2.3.4.1. Ubicación de las instalaciones

La seguridad comienza incluso antes de construir o adquirir un edificio. La ubicación geográfica influye directamente sobre el nivel de riesgo al que estará expuesta la organización.

Por ejemplo, un edificio situado en una zona con frecuentes inundaciones requerirá medidas de protección adicionales respecto de otro ubicado en un terreno elevado. Del mismo modo, instalar un centro de datos próximo a industrias químicas, estaciones de servicio o depósitos de materiales inflamables incrementa el riesgo ante posibles accidentes.

Al seleccionar una ubicación también conviene considerar aspectos como:

- estabilidad del terreno;
- riesgo sísmico;
- proximidad a ríos o cursos de agua;
- disponibilidad del suministro eléctrico;
- accesibilidad para servicios de emergencia;
- nivel de seguridad de la zona.

Estas variables suelen analizarse durante la planificación de nuevas instalaciones o cuando una organización decide trasladar su infraestructura tecnológica.

2.3.4.2. Estado de conservación del edificio

Una instalación deteriorada representa un riesgo para las personas y para los activos de información. Por esta razón, el mantenimiento preventivo constituye una parte importante de la Seguridad Física.

Algunas tareas habituales incluyen:

- inspección de techos;
- revisión de puertas y ventanas;
- reparación de filtraciones;
- mantenimiento de instalaciones eléctricas;
- verificación de sistemas de iluminación;
- revisión de sistemas hidráulicos.

Muchas organizaciones concentran sus esfuerzos en proteger los equipos informáticos, olvidando que una simple filtración de agua puede ocasionar daños mucho mayores que un ataque informático.

2.3.4.3. Iluminación

Una iluminación adecuada cumple dos funciones principales.

En primer lugar, mejora la seguridad de las personas al reducir la probabilidad de accidentes dentro de las instalaciones. En segundo lugar, actúa como un mecanismo disuasorio frente a intentos de intrusión, especialmente durante horarios nocturnos.

Las zonas de acceso, estacionamientos, depósitos y perímetros exteriores deberían disponer de iluminación suficiente para facilitar la vigilancia y el funcionamiento de los sistemas de videovigilancia.

2.3.4.4. Señalización

Toda organización debe disponer de señalización clara que permita identificar:

- salidas de emergencia;
- rutas de evacuación;
- ubicación de extintores;
- zonas restringidas;
- puntos de reunión;
- equipos de primeros auxilios.

Una correcta señalización facilita la respuesta ante situaciones de emergencia y reduce el riesgo de accidentes durante una evacuación.

2.3.4.5. Orden y limpieza

Aunque suele asociarse con cuestiones de mantenimiento, el orden constituye una medida de Seguridad Física. La acumulación de cajas, cables o materiales inflamables puede dificultar la evacuación de personas, favorecer la propagación de incendios o provocar accidentes laborales.

Mantener las áreas de trabajo ordenadas también facilita la detección de objetos extraños o manipulaciones no autorizadas.

2.3.4.6. Mantenimiento preventivo

La infraestructura debe inspeccionarse periódicamente para detectar fallas antes de que produzcan incidentes.

Entre las tareas más frecuentes pueden mencionarse:

- revisión de instalaciones eléctricas;
- mantenimiento de puertas automáticas;
- verificación de cerraduras;
- inspección de detectores de humo;
- prueba de sistemas de iluminación de emergencia;
- revisión de canalizaciones de agua.

El mantenimiento preventivo suele resultar considerablemente menos costoso que la reparación de daños ocasionados por una falla inesperada.

2.3.5. Ejemplo de aplicación

2.3.5.1. Protección de instalaciones en una entidad bancaria

Las entidades bancarias manejan información altamente sensible y almacenan importantes valores económicos, por lo que requieren elevados niveles de protección física.

Entre las medidas habitualmente implementadas se encuentran:

- edificios construidos con materiales resistentes;
- accesos claramente definidos;
- iluminación perimetral;
- puertas de seguridad;
- vidrios reforzados;
- áreas restringidas para servidores;
- sistemas de videovigilancia permanente;
- mantenimiento preventivo de las instalaciones.

Estas medidas buscan reducir tanto el riesgo de intrusión como las consecuencias derivadas de incidentes accidentales.

Aunque una universidad o una empresa comercial no requieren el mismo nivel de protección que un banco, muchas de estas medidas pueden adaptarse a cualquier organización.

2.4. Áreas Seguras y Perímetros de Seguridad
2.4.1. Introducción

No todas las dependencias de una organización requieren el mismo nivel de protección. Mientras que algunas áreas son de libre acceso para empleados y visitantes, otras contienen activos cuya pérdida o daño podría comprometer seriamente el funcionamiento de la organización.

Por esta razón, uno de los principios fundamentales de la Seguridad Física consiste en dividir las instalaciones en diferentes zonas según el nivel de protección requerido. Esta división permite establecer controles específicos para cada espacio, limitando el acceso únicamente al personal autorizado y reduciendo la exposición de los activos más críticos.

En este contexto aparecen dos conceptos estrechamente relacionados: las **áreas seguras** y los **perímetros de seguridad**. Las áreas seguras identifican aquellos espacios que requieren un nivel especial de protección, mientras que los perímetros de seguridad constituyen las barreras físicas que delimitan y resguardan dichas áreas.

En los siguientes apartados se analizarán ambos conceptos y se estudiará cómo contribuyen a proteger la infraestructura y la información de una organización.

2.4.2. Concepto de Áreas Seguras

Una organización está compuesta por diferentes espacios físicos donde se desarrollan actividades administrativas, técnicas y operativas. Sin embargo, no todas estas áreas poseen la misma importancia desde el punto de vista de la seguridad.

Mientras que algunas zonas pueden ser utilizadas libremente por empleados o visitantes, otras albergan equipos críticos, documentación confidencial o infraestructura esencial para el funcionamiento de la organización. Estas últimas requieren medidas especiales de protección y reciben el nombre de **áreas seguras**.

Un área segura es un espacio físico al que únicamente pueden acceder personas expresamente autorizadas, debido a que contiene activos cuya pérdida, alteración o destrucción produciría un impacto significativo sobre la organización.

El objetivo principal de un área segura consiste en reducir la probabilidad de que personas no autorizadas puedan acceder a recursos críticos, ya sea de manera accidental o intencional.

Entre los ejemplos más comunes de áreas seguras pueden mencionarse:

- Centros de cómputos.
- Salas de servidores.
- Centros de procesamiento de información.
- Salas de comunicaciones.
- Archivos con documentación confidencial.

- Salas donde se almacenan copias de seguridad.
- Laboratorios de investigación.
- Salas de monitoreo y control.

El nivel de protección aplicado dependerá del valor de los activos contenidos en cada una de estas áreas.

2.4.2.1. Características de un Área Segura

Aunque las características específicas varían según el tipo de organización, la mayoría de las áreas seguras presentan elementos comunes destinados a controlar el acceso y proteger los activos.

Entre las características más habituales se encuentran:

- acceso restringido únicamente al personal autorizado;
- registro de ingresos y egresos;
- puertas con sistemas de cierre seguro;
- videovigilancia permanente;
- protección contra incendios;
- protección eléctrica;
- monitoreo ambiental;
- señalización adecuada.

Es importante destacar que un área segura no necesariamente corresponde a una habitación completamente aislada. También puede tratarse de un sector específico dentro de una oficina o de una zona delimitada mediante controles de acceso.

Por ejemplo, en una universidad, la sala donde se encuentran los servidores institucionales constituye un área segura, mientras que las oficinas administrativas pueden ser consideradas áreas de acceso general para el personal.

2.4.2.2. Clasificación de las Áreas según su nivel de acceso

Muchas organizaciones clasifican sus instalaciones en diferentes niveles de seguridad con el propósito de facilitar la administración de los permisos de acceso.

Una clasificación sencilla podría ser la siguiente.

Nivel	Tipo de acceso	Ejemplos
Público	Acceso libre	Recepción, sala de espera
Interno	Solo empleados	Oficinas administrativas
Restringido	Personal autorizado	Área de informática
Crítico	Acceso altamente controlado	Centro de Datos

Esta clasificación permite aplicar controles proporcionales al nivel de criticidad de cada área. No tendría sentido exigir autenticación biométrica para ingresar a una sala de reuniones utilizada por visitantes, pero sí resulta razonable implementarla en el acceso a un centro de cómputos.

2.4.3. Concepto de Perímetro de Seguridad

Una vez definidas las áreas que requieren protección especial, resulta necesario establecer mecanismos destinados a impedir el acceso no autorizado.

Aquí aparece el concepto de **perímetro de seguridad**.

Un perímetro de seguridad es el límite físico que delimita un área protegida y sobre el cual se implementan controles destinados a detectar, retrasar o impedir el ingreso de personas no autorizadas.

En otras palabras, el perímetro constituye la primera barrera de protección de un área segura.

Dependiendo de las características de la organización, el perímetro puede estar formado por distintos elementos, tales como:

- cercos;
- muros;
- puertas de seguridad;
- portones;
- rejas;
- torniquetes;
- esclusas de acceso.

Cuanto mayor sea la criticidad del área protegida, mayor será el nivel de seguridad requerido en su perímetro.

2.4.3.1. Funciones de un Perímetro de Seguridad

Los perímetros de seguridad cumplen diversas funciones dentro de una estrategia de protección física. Entre las más importantes pueden mencionarse:

Delimitar áreas protegidas

Permiten identificar claramente dónde comienza una zona restringida y dónde finaliza un área de acceso general. Esto facilita el establecimiento de políticas de acceso y la aplicación de controles específicos.

Disuadir intentos de intrusión

La simple presencia de barreras físicas visibles suele actuar como un elemento disuasorio frente a posibles intentos de acceso no autorizado. Una persona tiene menos probabilidades de intentar ingresar a un área protegida cuando observa controles claramente establecidos.

Retrasar al intruso

Aunque ningún sistema puede garantizar una protección absoluta, un buen perímetro incrementa el tiempo necesario para acceder a un área protegida. Ese tiempo adicional permite que otros mecanismos de seguridad, como las alarmas o el personal de vigilancia, detecten el incidente y respondan oportunamente.

Facilitar la supervisión

La existencia de accesos claramente definidos simplifica las tareas de vigilancia. En lugar de controlar múltiples puntos de ingreso, el personal de seguridad puede concentrar sus esfuerzos en un número reducido de accesos autorizados.

2.4.4. Relación entre Áreas Seguras y Perímetros de Seguridad

Estos dos conceptos suelen confundirse, aunque representan elementos diferentes dentro de la Seguridad Física.

Un área segura constituye el espacio que requiere protección.

El perímetro de seguridad corresponde al límite físico que protege dicha área.

En este ejemplo, el centro de cómputos constituye el área segura, mientras que la puerta reforzada, el sistema de control de acceso y las barreras físicas delimitan el perímetro que protege dicho espacio.

Esta diferenciación resulta importante porque muchas organizaciones implementan controles de acceso sofisticados dentro del área segura, pero descuidan el perímetro exterior, facilitando que personas no autorizadas alcancen zonas críticas.

2.4.5. Ejemplo de aplicación

Una empresa de telecomunicaciones posee un edificio de cuatro plantas. La planta baja alberga la recepción y las oficinas de atención al cliente, por lo que el acceso está permitido al público durante el horario comercial. En el segundo piso funcionan las oficinas administrativas, accesibles únicamente para empleados de la empresa mediante tarjeta de identificación. En el tercer piso se encuentra el centro de datos corporativo, considerado un área crítica. Para ingresar a esta sala es necesario atravesar un perímetro compuesto por una puerta de seguridad con cerradura electrónica, autenticación biométrica y registro automático de accesos.

Este ejemplo muestra cómo una misma organización puede definir diferentes niveles de protección según la importancia de los activos ubicados en cada espacio.

2.5. Control de Acceso Físico

2.5.1. Introducción

Hasta este momento se ha estudiado cómo proteger las instalaciones y cómo delimitar áreas críticas mediante perímetros de seguridad. Sin embargo, surge una pregunta fundamental:

¿Quién puede ingresar a esas áreas y bajo qué condiciones?

Responder esta pregunta constituye precisamente el objetivo del **control de acceso físico**.

El control de acceso físico comprende el conjunto de políticas, procedimientos y mecanismos destinados a regular el ingreso, permanencia y salida de personas, vehículos o materiales dentro de una instalación.

Su finalidad principal consiste en garantizar que únicamente las personas autorizadas puedan acceder a determinadas áreas, reduciendo la probabilidad de robos, sabotajes, daños accidentales o divulgación de información confidencial.

En organizaciones modernas, el control de acceso representa uno de los controles físicos más importantes, ya que constituye la primera barrera para proteger activos críticos como centros de datos, salas de comunicaciones, laboratorios y archivos confidenciales.

2.5.2. Concepto de Control de Acceso Físico

El control de acceso físico es el conjunto de medidas destinadas a verificar la identidad de una persona antes de permitir su ingreso a una instalación o a un área protegida, asegurando que únicamente quienes poseen autorización puedan acceder a ella.

Este proceso no consiste únicamente en abrir o cerrar una puerta. Implica una serie de actividades coordinadas que permiten responder cuatro preguntas fundamentales:

- ¿Quién intenta ingresar?
- ¿Está correctamente identificado?
- ¿Posee autorización para ingresar?
- ¿Debe quedar registrado el acceso?

Estas cuatro preguntas constituyen la base de cualquier sistema moderno de control de acceso.

2.5.3. Objetivos del Control de Acceso

Todo sistema de control de acceso busca cumplir los siguientes objetivos:

- Impedir el ingreso de personas no autorizadas;
- Restringir el acceso únicamente a quienes lo necesiten para realizar sus funciones;
- Registrar los accesos realizados;
- Proteger activos críticos;
- Facilitar investigaciones posteriores ante incidentes;
- Cumplir requisitos legales y normativos relacionados con la seguridad.

2.5.4. El proceso de control de acceso

Aunque existen numerosas tecnologías para controlar accesos, todas ellas siguen un proceso similar compuesto por cuatro etapas.

1. Identificación

La persona comunica al sistema quién afirma ser.

Por ejemplo:

- Presenta una credencial;
- Acerca una tarjeta RFID;
- Introduce un número de identificación;
- Informa su nombre al personal de seguridad.

La identificación no demuestra que la persona sea realmente quien dice ser; únicamente proporciona una identidad.

2. Autenticación

En esta etapa el sistema verifica que la identidad declarada sea verdadera.

La autenticación puede realizarse mediante distintos mecanismos, como:

- Contraseña;
- Tarjeta inteligente;
- Huella digital;
- Reconocimiento facial;
- Reconocimiento del iris;
- Combinación de varios factores.

La autenticación reduce significativamente la probabilidad de suplantación de identidad.

3. Autorización

Una vez autenticada la identidad, el sistema determina si esa persona posee permiso para ingresar al área solicitada.

Por ejemplo, un técnico de redes puede estar autorizado para ingresar a la sala de comunicaciones, pero no al archivo donde se almacenan documentos financieros.

La autorización depende de las políticas de seguridad definidas por la organización.

4. Registro

Finalmente, el sistema registra el evento.

Generalmente almacena información como:

- Identidad de la persona;
- Fecha;
- Hora;
- Puerta utilizada;
- Resultado del acceso (autorizado o denegado).

Estos registros constituyen evidencia importante durante auditorías e investigaciones de incidentes.

2.5.5. El principio de mínimo privilegio aplicado al acceso físico

Uno de los principios fundamentales de la seguridad consiste en **otorgar únicamente los permisos estrictamente necesarios para realizar una tarea**. Este principio, conocido como **mínimo privilegio**, también se aplica al acceso físico.

Por ejemplo:

- El personal administrativo no necesita ingresar al centro de cómputos.
- Los visitantes no deberían acceder sin supervisión a áreas técnicas.
- El personal de limpieza puede requerir acceso únicamente en horarios específicos y bajo determinadas condiciones.
- Los proveedores externos deberían acceder exclusivamente al área donde realizarán su trabajo.

Limitar los permisos reduce considerablemente la superficie de exposición y disminuye la probabilidad de incidentes derivados de errores humanos o acciones maliciosas.

2.5.6. Mecanismos de Control de Acceso

Una vez definido el procedimiento de identificación, autenticación, autorización y registro, la organización debe seleccionar los mecanismos mediante los cuales controlará el ingreso de personas a sus instalaciones.

No existe un único sistema válido para todas las organizaciones. La elección dependerá del nivel de criticidad del área protegida, del presupuesto disponible, de la cantidad de usuarios y del nivel de riesgo aceptable.

Desde el punto de vista de la autenticación, los mecanismos de control de acceso pueden clasificarse según el factor utilizado para verificar la identidad de una persona.

Tradicionalmente se distinguen tres grandes categorías:

- Algo que la persona **posee**.
- Algo que la persona **conoce**.
- Algo que la persona **es**.

En los últimos años también han surgido otros factores, como la ubicación geográfica o el comportamiento del usuario, aunque en Seguridad Física predominan los tres primeros.

2.5.6.1. Autenticación basada en algo que la persona posee

En este tipo de autenticación el usuario demuestra su identidad presentando un objeto físico previamente asignado por la organización.

Los mecanismos más utilizados son:

- Credenciales impresas;
- Tarjetas magnéticas;
- Tarjetas RFID;
- Tarjetas inteligentes (smart cards);
- Llaves electrónicas;
- Tokens de proximidad.

La ventaja principal consiste en su facilidad de utilización y administración.

Sin embargo, presentan un inconveniente evidente: pueden perderse, ser robadas o prestadas a otras personas.

Por esta razón, las organizaciones con mayores exigencias de seguridad suelen complementar este mecanismo con otros factores de autenticación.

Credenciales

Una **credencial** es un documento físico o electrónico que identifica a una persona y demuestra su pertenencia a una organización.

Generalmente contiene información como:

- Fotografía;
- Nombre y apellido;
- Número de identificación;
- Cargo;
- Área de trabajo;
- Empresa;
- Fecha de vencimiento;
- Código QR o chip RFID.

En muchas organizaciones la credencial cumple una doble función. Por un lado, identifica visualmente al empleado. Por otro lado, permite habilitar automáticamente el acceso mediante lectores electrónicos.

Tipos de credenciales

Dependiendo de la tecnología utilizada, pueden distinguirse diferentes tipos.

Credenciales impresas

Son las más sencillas. Consisten en tarjetas plásticas con fotografía y datos personales. Su función principal es identificar visualmente al portador. Generalmente requieren la intervención de personal de seguridad para autorizar el ingreso.

Tarjetas con banda magnética

Incorporan una banda similar a la utilizada antiguamente en las tarjetas bancarias. Para acceder es necesario deslizar la tarjeta por un lector. Actualmente su utilización ha disminuido debido al desgaste de la banda y a la aparición de tecnologías más modernas.

Tarjetas RFID

Las tarjetas RFID (Radio Frequency Identification) utilizan ondas de radio para transmitir un código de identificación. No es necesario introducir la tarjeta en un lector. Simplemente debe acercarse a una distancia determinada. Actualmente constituyen uno de los mecanismos más utilizados en edificios corporativos y universidades.

Tarjetas inteligentes (Smart Cards)

Incorporan un microprocesador capaz de almacenar información y ejecutar operaciones criptográficas. Además de controlar accesos físicos pueden utilizarse para:

- Autenticación informática;
- Firma digital;
- Acceso a sistemas internos;
- Certificados digitales.

Representan una alternativa mucho más segura que las tarjetas tradicionales.

Ventajas de las credenciales

Entre sus principales ventajas pueden mencionarse:

- facilidad de uso;
- rapidez de acceso;
- bajo costo de implementación;
- integración con sistemas informáticos;
- registro automático de ingresos.

Desventajas

También presentan algunas limitaciones.

Las más importantes son:

- pérdida de la credencial;
- robo;
- préstamo entre empleados;
- duplicación en algunos sistemas antiguos;
- deterioro por uso.

Estas limitaciones explican por qué las organizaciones de alta seguridad suelen combinar las credenciales con mecanismos biométricos.

2.5.6.2. Autenticación basada en algo que la persona conoce

En este caso la autenticación depende de un conocimiento que únicamente debería poseer el usuario.

Los mecanismos más comunes son:

- PIN;
- contraseña;
- código numérico;
- patrón de desbloqueo.

Aunque son ampliamente utilizados en sistemas informáticos, también aparecen en Seguridad Física.

Por ejemplo:

- Teclados numéricos para abrir puertas;
- Cajas fuertes;
- Armarios de seguridad;
- Salas técnicas.

Su principal ventaja es que no requieren dispositivos físicos. Sin embargo, presentan importantes desventajas.

Las personas pueden:

- Olvidar el código;
- Escribirlo en lugares visibles;
- Compartirlo con otros usuarios;
- Elegir combinaciones fáciles de adivinar.

Por ello, rara vez se utilizan como único mecanismo para proteger áreas críticas.

2.5.6.3. Autenticación basada en algo que la persona es

Este mecanismo utiliza características físicas o comportamentales propias de cada individuo. Recibe el nombre de **autenticación biométrica**.

Actualmente representa uno de los métodos más seguros para controlar accesos físicos.

La biometría se basa en la idea de que ciertas características humanas poseen un elevado grado de unicidad y pueden emplearse para verificar la identidad de una persona.

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.

A diferencia de una contraseña o una tarjeta, las características biométricas forman parte del propio individuo. Por ello no pueden olvidarse ni prestarse a otra persona.

Funcionamiento general

Aunque existen diversas tecnologías biométricas, todas siguen un proceso similar.

Primera etapa: Registro (Enrollment)

Cuando una persona ingresa por primera vez al sistema, se capturan sus características biométricas.

Por ejemplo:

- Huella digital;
- Rostro;
- Iris.

El sistema genera una plantilla matemática.

Es importante aclarar que normalmente **no almacena una fotografía completa**, sino una representación matemática de las características principales.

Segunda etapa: Verificación

Cada vez que el usuario intenta ingresar, el sistema captura nuevamente la característica biométrica. Posteriormente compara dicha información con la plantilla almacenada. Si ambas coinciden dentro de un margen aceptable, el acceso es autorizado.

Principales tecnologías biométricas

Huella digital

Es la tecnología biométrica más difundida. Su funcionamiento se basa en el análisis de las crestas y valles presentes en las yemas de los dedos.

Ventajas

- Rápida;
- Económica;
- Ampliamente aceptada;
- Elevada precisión.

Desventajas

- Suciedad o humedad pueden dificultar la lectura;
- Lesiones en los dedos;
- Desgaste en determinados trabajos manuales.

Reconocimiento facial

Analiza características geométricas del rostro. Actualmente muchos sistemas utilizan inteligencia artificial para mejorar la precisión.

Ventajas

- No requiere contacto físico;
- Alta comodidad;
- Integración con CCTV.

Desventajas

- Iluminación deficiente;
- Uso de mascarillas;
- Cambios importantes en la apariencia.

Reconocimiento del iris

Analiza el patrón del iris humano. Es considerado uno de los métodos biométricos más precisos.

Ventajas

- Muy baja probabilidad de error;
- Extremadamente difícil de falsificar.

Desventajas

- Costo elevado;
- Equipos especializados.

Geometría de la mano

Analiza dimensiones generales de la mano. Aunque fue ampliamente utilizada durante muchos años, actualmente ha sido reemplazada en gran medida por la huella digital y el reconocimiento facial.

Reconocimiento de voz

Analiza características particulares de la voz. Su uso es más frecuente en sistemas telefónicos que en control de acceso físico.

Comparación de tecnologías biométricas

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

2.5.6.4. Autenticación multifactor

En instalaciones críticas es recomendable combinar varios factores de autenticación.

Por ejemplo:

- Tarjeta RFID + huella digital;
- Credencial + PIN;
- Reconocimiento facial + tarjeta inteligente.

Este enfoque recibe el nombre de **autenticación multifactor (MFA)** y proporciona un nivel de seguridad considerablemente superior al uso de un único mecanismo. Un atacante podría robar una credencial, pero le resultaría mucho más difícil falsificar simultáneamente una característica biométrica del usuario legítimo.

2.5.7. Ejemplo de aplicación
2.5.7.1. Control de acceso en una empresa tecnológica

Una empresa dedicada al desarrollo de software ocupa un edificio de cinco plantas. El acceso principal se realiza mediante torniquetes equipados con lectores RFID. Cada empleado utiliza una tarjeta de proximidad para ingresar al edificio. Las áreas administrativas requieren únicamente la presentación de la credencial.

Sin embargo, el acceso al centro de datos exige autenticación multifactor:

- Tarjeta RFID;
- Reconocimiento de huella digital.

Todas las puertas permanecen conectadas al sistema central de seguridad.

Cada intento de acceso queda registrado junto con:

- identidad del usuario;
- fecha;
- hora;
- puerta utilizada;
- resultado del intento.

Las cámaras CCTV comienzan a grabar automáticamente cuando se produce un acceso fuera del horario laboral.

Gracias a esta integración, la organización puede conocer en todo momento quién ingresó a cada área y detectar rápidamente cualquier comportamiento anómalo.

2.5.8. Relación del Control de Acceso con otros apartados de la unidad

Hasta este momento se han desarrollado tres elementos fundamentales de la Seguridad Física:

- la protección de las instalaciones;
- la definición de áreas seguras y perímetros;
- el control de acceso físico.

Estos controles tienen una finalidad preventiva: impedir que personas no autorizadas alcancen los activos críticos. Sin embargo, ningún sistema de protección puede garantizar un nivel absoluto de seguridad. Siempre existe la posibilidad de que un intruso intente vulnerar los controles o que ocurra un incidente inesperado. Por esta razón, resulta necesario incorporar mecanismos capaces de detectar eventos anómalos y alertar rápidamente al personal responsable.

Dos de las tecnologías más utilizadas para cumplir esta función son los sistemas de videovigilancia y los sistemas de alarmas, que se estudiarán en el siguiente apartado.

2.5.9. Sistemas de Videovigilancia (CCTV) y Sistemas de Alarmas

2.5.9.1. Introducción

La protección de una instalación no depende únicamente de impedir el acceso de personas no autorizadas. También es necesario contar con mecanismos que permitan observar lo

que sucede dentro y fuera de las instalaciones, detectar comportamientos sospechosos y generar alertas cuando ocurre un incidente.

En este contexto, los sistemas de videovigilancia y los sistemas de alarmas desempeñan un papel fundamental dentro de la Seguridad Física.

Aunque ambos persiguen objetivos diferentes, suelen trabajar de manera integrada. Mientras que el sistema de videovigilancia proporciona información visual sobre los acontecimientos que ocurren en la instalación, los sistemas de alarmas detectan situaciones anormales y notifican inmediatamente al personal responsable para que pueda actuar. La combinación de ambas tecnologías permite mejorar significativamente la capacidad de prevención, detección y respuesta frente a incidentes de seguridad.

2.5.9.2. Sistemas de Videovigilancia (CCTV)

Concepto

El término **CCTV** proviene de la expresión inglesa **Closed Circuit Television** (Televisión de Circuito Cerrado).

Un sistema CCTV es un conjunto de cámaras, dispositivos de grabación, equipos de comunicación y software destinado a capturar, transmitir, almacenar y visualizar imágenes de determinadas áreas con fines de seguridad.

Se denomina "circuito cerrado" porque las imágenes no se transmiten al público en general, sino únicamente a un conjunto limitado de dispositivos autorizados dentro de la organización. Actualmente, los sistemas CCTV representan uno de los controles físicos más utilizados para proteger edificios corporativos, industrias, hospitales, universidades, bancos, centros comerciales y centros de datos.

Objetivos de un sistema CCTV

La instalación de un sistema de videovigilancia persigue diversos objetivos, entre los que pueden destacarse:

- Supervisar permanentemente áreas críticas;
- Disuadir conductas delictivas;
- Detectar accesos no autorizados;
- Registrar incidentes para su posterior análisis;
- Facilitar investigaciones internas;
- Proporcionar evidencia ante procesos judiciales;
- Apoyar al personal de seguridad durante situaciones de emergencia.

Es importante destacar que un sistema CCTV no reemplaza otros mecanismos de seguridad, sino que los complementa. Por ejemplo, una cámara puede registrar el ingreso de una persona no autorizada, pero no impide físicamente dicho ingreso. Para ello resulta indispensable la existencia de controles de acceso adecuados.

Componentes de un sistema CCTV

Aunque existen numerosas configuraciones posibles, la mayoría de los sistemas de videovigilancia están compuestos por los siguientes elementos.

Cámaras

Son los dispositivos encargados de capturar las imágenes. Actualmente predominan las cámaras digitales IP, que transmiten la información a través de redes informáticas y permiten alcanzar altas resoluciones. Dependiendo de las necesidades de la organización, pueden instalarse cámaras fijas o cámaras motorizadas con capacidad de giro, inclinación y zoom.

Grabadores

Las imágenes captadas por las cámaras deben almacenarse para su posterior consulta.

Esta función puede realizarse mediante:

- DVR (Digital Video Recorder), utilizado principalmente con cámaras analógicas;
- NVR (Network Video Recorder), empleado en sistemas basados en cámaras IP.

Estos dispositivos permiten conservar grabaciones durante un período determinado, facilitando la investigación de incidentes.

Monitores

Permiten visualizar en tiempo real las imágenes captadas por las cámaras. Generalmente se encuentran en los puestos del personal de vigilancia o en los centros de monitoreo.

Software de gestión

El software centraliza la administración del sistema y permite realizar tareas como:

- Visualizar cámaras en tiempo real;
- Reproducir grabaciones;
- Buscar eventos específicos;
- Generar alertas;
- Administrar usuarios;
- Controlar cámaras;
- Integrar el sistema con otros controles de seguridad.

Infraestructura de comunicaciones

Las cámaras deben transmitir las imágenes hacia los equipos de grabación y monitoreo. Esta comunicación puede realizarse mediante:

- Cableado estructurado;
- Fibra óptica;
- Redes inalámbricas;
- Redes dedicadas de videovigilancia.

La elección dependerá del tamaño de la instalación y de los requerimientos de ancho de banda.

2.5.9.3. Ejemplo de aplicación

Una empresa logística posee un depósito de aproximadamente diez mil metros cuadrados donde se almacenan productos de alto valor.

Para mejorar la seguridad se diseñó un sistema CCTV compuesto por:

- Cámaras fijas en los accesos;
- Cámaras en el depósito principal;
- Cámaras térmicas en el perímetro exterior;
- Software de análisis inteligente para detectar movimientos fuera del horario laboral;
- Almacenamiento redundante de las grabaciones durante sesenta días.

El sistema se integró con el control de acceso y las alarmas de intrusión.

Cuando una persona intenta ingresar fuera del horario autorizado, el software realiza automáticamente las siguientes acciones:

1. Registra el evento;
2. Activa la cámara más cercana;
3. Genera una alerta en el centro de monitoreo;
4. Envía una notificación al personal de seguridad.

Esta integración permite reducir significativamente el tiempo de respuesta ante posibles incidentes.

2.5.10. Sistemas de Alarmas
2.5.10.1. Concepto

Las organizaciones incorporan mecanismos capaces de **detectar automáticamente situaciones anómalas** y **notificar inmediatamente al personal responsable**, permitiendo una respuesta rápida antes de que el incidente produzca daños importantes.

Estos mecanismos reciben el nombre de **sistemas de alarmas**.

Un **sistema de alarmas** es el conjunto de dispositivos electrónicos y procedimientos destinados a detectar automáticamente condiciones anormales o peligrosas y generar una señal de advertencia para que puedan adoptarse las medidas necesarias.

Dependiendo del tipo de riesgo que se pretenda controlar, un sistema de alarmas puede detectar:

- Accesos no autorizados;
- Apertura indebida de puertas o ventanas;
- Movimientos en áreas restringidas;
- Presencia de humo;
- Aumento anormal de temperatura;
- Fugas de agua;
- Cortes del suministro eléctrico;
- Fallas en equipos críticos;
- Presencia de gases peligrosos.

Una característica importante de estos sistemas es que **no actúan directamente sobre la amenaza**, sino que proporcionan una advertencia temprana que permite minimizar las consecuencias del incidente.

En otras palabras, una alarma no evita un incendio ni impide un robo; su función consiste en detectar el evento lo antes posible para que la organización pueda responder rápidamente.

2.5.10.2. Funcionamiento general de un sistema de alarmas

Aunque existen numerosos tipos de alarmas, la mayoría de los sistemas modernos siguen un esquema de funcionamiento similar.

El proceso puede dividirse en cuatro etapas.

1. Detección

Un sensor identifica una condición anormal.

Por ejemplo:

- Apertura de una puerta;
- Movimiento;
- Presencia de humo;
- Incremento de temperatura;
- Corte del suministro eléctrico.

2. Procesamiento

La información enviada por el sensor es recibida por una central de control. Esta central determina si la condición detectada constituye realmente un evento que requiere generar una alarma.

Por ejemplo, un movimiento detectado fuera del horario laboral puede interpretarse como un posible intento de intrusión, mientras que el mismo movimiento durante el horario de atención puede considerarse normal.

3. Generación de la alarma

Si la condición cumple los criterios establecidos, el sistema genera una alerta.

Dependiendo de la configuración, la alarma puede consistir en:

- Una sirena sonora;
- Una luz estroboscópica;
- Un mensaje en la consola de monitoreo;
- Una llamada telefónica automática;
- Un correo electrónico;
- Una notificación en una aplicación móvil.

4. Respuesta

Finalmente, el personal responsable evalúa la situación y aplica el procedimiento correspondiente.

La respuesta puede incluir:

- Verificar las imágenes del sistema CCTV;
- Enviar personal de seguridad;
- Evacuar el edificio;
- Contactar a bomberos;
- Cortar el suministro eléctrico;
- Activar el plan de contingencia.

Esta última etapa es fundamental, ya que una alarma solo resulta útil cuando existe un procedimiento previamente definido para responder al incidente.

2.5.10.3. Tipos de Sistemas de Alarmas

Los sistemas de alarmas pueden clasificarse según el tipo de amenaza que están diseñados para detectar. Aunque todos persiguen el mismo objetivo —detectar situaciones anormales y alertar al personal responsable—, cada uno utiliza sensores específicos y responde a riesgos diferentes.

En Seguridad Física, los sistemas de alarmas más utilizados son:

- Alarmas de intrusión;
- Alarmas contra incendios;
- Alarmas ambientales;
- Alarmas técnicas.

Alarmas de Intrusión

Concepto

Las **alarmas de intrusión** son sistemas diseñados para detectar intentos de acceso no autorizado a una instalación o a un área protegida. Su finalidad consiste en advertir rápidamente la presencia de personas que intentan ingresar sin autorización, permitiendo que el personal de seguridad intervenga antes de que se produzcan daños o robos.

Normalmente este tipo de alarmas permanece activo fuera del horario laboral o en áreas donde el acceso debe permanecer permanentemente restringido, como los centros de datos.

Sensores utilizados

Las alarmas de intrusión pueden incorporar diferentes tipos de sensores.

Detectores de movimiento

Detectan desplazamientos dentro de un área protegida. La mayoría utiliza sensores infrarrojos pasivos (PIR), aunque también existen sensores de microondas o sistemas que combinan ambas tecnologías para reducir falsas alarmas.

Contactos magnéticos

Están formados por dos piezas:

- un imán;
- un interruptor magnético (reed switch).

Cuando una puerta o ventana se abre, ambas piezas se separan y el sistema detecta la apertura.

Detectores de rotura de cristales

Estos sensores identifican el sonido o la vibración producida cuando se rompe un vidrio.

Sensores sísmicos o de vibración

Detectan golpes, perforaciones o vibraciones anormales.

Barreras infrarrojas

Consisten en un emisor y un receptor que generan un haz infrarrojo invisible. Cuando una persona atraviesa dicho haz, el sistema interpreta la interrupción como un posible intento de intrusión.

Alarmas contra Incendios

Concepto

Las **alarmas contra incendios** son sistemas destinados a detectar de manera temprana las condiciones que pueden indicar el inicio de un incendio, permitiendo alertar rápidamente a los ocupantes del edificio y activar los procedimientos de emergencia.

Su principal objetivo consiste en proteger la vida de las personas y reducir los daños materiales ocasionados por el fuego.

A diferencia de las alarmas de intrusión, cuyo propósito es detectar accesos no autorizados, las alarmas contra incendios buscan identificar fenómenos físicos asociados al proceso de combustión.

Principales detectores

Dependiendo del tipo de instalación, pueden emplearse distintos dispositivos.

Detectores de humo

Son los más utilizados. Permiten detectar las partículas generadas durante las primeras etapas de un incendio, incluso antes de que aparezcan llamas visibles. Existen dos tecnologías principales:

- Detectores fotoeléctricos;
- Detectores por ionización.

Detectores de temperatura

Se activan cuando la temperatura supera un determinado valor o aumenta rápidamente. Son apropiados para ambientes donde el humo forma parte del funcionamiento normal de la instalación, como cocinas industriales o talleres.

Detectores de llama

Detectan la radiación emitida por una llama mediante sensores ultravioleta o infrarrojos. Se utilizan especialmente en instalaciones industriales donde existe riesgo de incendios de rápida propagación.

2.6. Protección contra Incendios

2.6.1. Concepto

La **protección contra incendios** comprende el conjunto de medidas preventivas, sistemas de detección, mecanismos de extinción y procedimientos de actuación destinados a reducir la probabilidad de que se produzca un incendio, limitar su propagación y minimizar sus consecuencias sobre las personas, las instalaciones y los activos de la organización.

Es importante comprender que la protección contra incendios no consiste únicamente en disponer de extintores. Una estrategia eficaz combina diversas medidas que actúan antes, durante y después del inicio del fuego.

Entre ellas pueden mencionarse:

- Prevención de las causas que originan incendios;
- Diseño seguro de las instalaciones;
- Detección temprana;
- Sistemas automáticos de extinción;
- Medios manuales de combate del fuego;
- Planes de evacuación;
- Capacitación del personal.

La combinación de estos elementos permite reducir considerablemente el riesgo asociado a esta amenaza.

2.6.2. Concepto de fuego

El **fuego** es una reacción química de oxidación rápida, denominada **combustión**, que libera calor, luz y diversos productos de la combustión, como gases y humo.

Para que esta reacción pueda mantenerse deben reunirse determinadas condiciones físicas y químicas. Cuando el fuego permanece controlado y cumple una finalidad útil, como ocurre en una cocina o en un horno industrial, no representa necesariamente un peligro. Sin embargo, cuando pierde el control y se propaga de manera no deseada, se transforma en un incendio.

2.6.3. Concepto de incendio

Un **incendio** es un fuego no controlado que se propaga libremente, poniendo en peligro la vida de las personas, las instalaciones, los bienes materiales o el medio ambiente. La principal diferencia entre ambos conceptos radica en el control.

Un fuego puede formar parte del funcionamiento normal de una actividad. Un incendio, en cambio, constituye siempre una situación de emergencia que requiere una respuesta inmediata.

Por ejemplo:

- La llama de una cocina industrial corresponde a un fuego controlado;
- Esa misma llama propagándose hacia cortinas o mobiliario constituye un incendio.

Distinguir ambos conceptos permite comprender por qué muchas medidas de Seguridad Física se orientan a impedir que un fuego inicialmente controlado evolucione hacia un incendio.

2.6.4. El Triángulo del Fuego

Uno de los conceptos fundamentales de la protección contra incendios es el **triángulo del fuego**.

Este modelo explica que para que exista combustión deben estar presentes simultáneamente tres elementos esenciales:

- Combustible;
- Comburente;
- Calor.

2.6.4.1. Combustible

Es toda sustancia capaz de arder. Puede presentarse en estado sólido, líquido o gaseoso.

Ejemplos:

- Papel;
- Madera;
- Plásticos;
- Telas;
- Combustibles líquidos;
- Gas natural;
- Pinturas;
- Solventes.

En una organización informática también actúan como combustibles:

- Cableado eléctrico;
- Mobiliario;
- Pisos técnicos;
- Documentación en papel;
- Aislantes plásticos de los equipos.

2.6.4.2. Comburente

El comburente es la sustancia que permite que la combustión continúe. En la mayoría de los incendios el comburente es el oxígeno presente en el aire atmosférico. Sin una concentración suficiente de oxígeno, la combustión no puede mantenerse.

2.6.4.3. Calor

El calor proporciona la energía necesaria para iniciar el proceso de combustión. Puede originarse por diversas causas, entre ellas:

- Cortocircuitos;
- Sobrecargas eléctricas;
- Chispas;
- Llamas abiertas;
- Superficies calientes;
- Fricción;
- Descargas eléctricas;
- Reacciones químicas.

La eliminación de cualquiera de estos tres elementos interrumpe la combustión.

Precisamente sobre este principio se basan los diferentes métodos de extinción que se estudiarán más adelante.

2.6.5. El Tetraedro del Fuego

Durante muchos años, el modelo del triángulo del fuego fue suficiente para explicar el proceso de combustión. Sin embargo, los avances en el estudio del comportamiento del fuego demostraron que la presencia de combustible, comburente y calor no era suficiente para mantener la combustión.

Se comprobó que era necesario un cuarto elemento: **la reacción química en cadena**.

Por esta razón surgió el modelo conocido como **tetraedro del fuego**, ampliamente utilizado en la actualidad por especialistas en prevención y protección contra incendios.

El tetraedro incorpora un cuarto elemento:

- Combustible;
- Comburente;
- Calor;
- **Reacción química en cadena**.

La reacción química en cadena consiste en una serie de reacciones que producen radicales libres altamente reactivos, los cuales mantienen la combustión de manera continua mientras existan los demás elementos.

En otras palabras, una vez iniciado el fuego, la propia combustión genera las condiciones necesarias para continuar propagándose.

Este concepto resulta especialmente importante porque explica el funcionamiento de determinados agentes extintores, como los extintores de polvo químico seco, que actúan interrumpiendo precisamente esta reacción en cadena.

De este modo, un incendio puede extinguirse eliminando cualquiera de los cuatro elementos del tetraedro:

- Retirando el combustible;
- Reduciendo la concentración de oxígeno;
- Disminuyendo la temperatura;
- Interrumpiendo la reacción química.

Esta clasificación constituye la base de todos los métodos modernos de extinción de incendios.

2.6.6. Clasificación de los incendios

No todos los incendios presentan las mismas características. El tipo de combustible involucrado determina la forma en que el fuego se comporta y, en consecuencia, el método de extinción más adecuado. Utilizar un agente extintor incorrecto puede agravar la situación o poner en peligro a quien intenta combatir el incendio.

Por este motivo, los incendios se clasifican en distintas categorías.

Aunque existen pequeñas diferencias entre las normas utilizadas en distintos países, la clasificación más difundida comprende las clases **A, B, C, D y K**.

2.6.6.1. Incendios Clase A

Corresponden a incendios que involucran materiales sólidos combustibles que, al quemarse, dejan brasas.

Ejemplos:

- Madera;
- Papel;
- Cartón;
- Telas;
- Muebles;
- Residuos sólidos.

Son los incendios más frecuentes en oficinas, escuelas y edificios administrativos. Generalmente pueden extinguirse utilizando agua o extintores multipropósito adecuados.

2.6.6.2. Incendios Clase B

Involucran líquidos inflamables o combustibles, así como gases inflamables.

Ejemplos:

- Nafta;
- Alcohol;
- Pinturas;
- Solventes;
- Aceites minerales;
- Gasoil;
- Gas licuado de petróleo.

En este tipo de incendios **no debe utilizarse agua a presión**, ya que puede favorecer la dispersión del combustible y aumentar la propagación del fuego.

Habitualmente se emplean espumas, dióxido de carbono (CO_2) o polvo químico seco.

2.6.6.3. Incendios Clase C

Se producen sobre equipos eléctricos energizados.

Ejemplos:

- Tableros eléctricos;
- Servidores;
- Ups;
- Computadoras;
- Impresoras;
- Cableado bajo tensión.

El principal riesgo consiste en la posibilidad de electrocución. Por esta razón deben utilizarse agentes extintores que no conduzcan la electricidad, como el dióxido de carbono o determinados polvos químicos secos.

Una vez eliminado el suministro eléctrico, el incendio deja de clasificarse como Clase C y pasa a corresponder a la clase del material que continúa ardiendo.

2.6.6.4. Incendios Clase D

Comprenden incendios producidos por metales combustibles.

Entre ellos pueden mencionarse:

- Magnesio;
- Sodio;
- Potasio;
- Titanio;
- Litio metálico.

Aunque son poco frecuentes en oficinas, pueden aparecer en determinados laboratorios o industrias. Requieren agentes extintores especiales, ya que el agua puede reaccionar violentamente con algunos de estos metales.

2.6.6.5. Incendios Clase K

Corresponden a incendios originados por aceites y grasas utilizados en cocinas industriales. Presentan características particulares debido a las elevadas temperaturas que alcanzan estos aceites. Su extinción requiere agentes químicos específicamente diseñados para este tipo de combustibles.

2.6.7. Extintores según tipo de incendios

A continuación, se presentan los tipos de extintores recomendados según el tipo de incendio:

Clase A: Fuegos de materiales combustibles ordinarios

Extintores recomendados:

- Agua (clase A)
- Espuma (clase A)
- Polvo químico seco (clase ABC)

Clase B: Fuegos de líquidos inflamables

Extintores recomendados:

- Espuma (clase B)
- Dióxido de carbono (clase B)
- Polvo químico seco (clase ABC)
- Agentes limpios (clase B)

Clase C: Fuegos de equipos eléctricos

Extintores recomendados:

- Dióxido de carbono (clase C)
- Polvo químico seco (clase ABC)
- Agentes limpios (clase C)

Clase D: Fuegos de metales combustibles

Extintores recomendados:

- Polvo químico seco especial para metales combustibles (clase D)

Clase K: Fuegos de aceites y grasas

Extintores recomendados:

- Agentes químicos húmedos (clase K)

Importante

- Nunca usar agua para apagar fuegos de clase B (líquidos inflamables) o clase C (equipos eléctricos), ya que puede empeorar la situación.
- Asegurarse de que el extintor esté cargado y sea adecuado para el tipo de fuego que estás enfrentando.
- Siempre seguir las instrucciones del fabricante y las recomendaciones de seguridad al usar un extintor de incendios.

2.7. Protección Eléctrica
2.7.1. Concepto y objetivos

La **protección eléctrica** comprende el conjunto de medidas, dispositivos y procedimientos destinados a garantizar un suministro eléctrico seguro y confiable, protegiendo tanto a las personas como a los equipos e instalaciones frente a fallas de origen eléctrico.

Una interrupción del servicio eléctrico o una falla en la instalación puede provocar desde la detención temporal de las actividades hasta la pérdida de información crítica, daños en equipos informáticos o incendios.

Desde el punto de vista de la **Seguridad Informática**, la protección eléctrica constituye un elemento fundamental para garantizar la **disponibilidad** de la información y la continuidad de los servicios.

2.7.2. Objetivos de la protección eléctrica

Los principales objetivos son:

- proteger la integridad física de las personas frente a accidentes eléctricos;
- prevenir incendios originados por fallas en las instalaciones;
- proteger los equipos informáticos y electrónicos contra daños eléctricos;
- garantizar la continuidad del suministro para los sistemas críticos;
- reducir el riesgo de pérdida o corrupción de la información;
- minimizar las interrupciones en las operaciones de la organización.

En definitiva, una adecuada protección eléctrica contribuye tanto a la seguridad de las personas como a la disponibilidad y continuidad de los sistemas de información.

2.7.3. Riesgos eléctricos

Las instalaciones eléctricas pueden verse afectadas por diferentes tipos de fallas que comprometen el funcionamiento normal de una organización.

Los riesgos eléctricos más frecuentes son los siguientes:

Riesgo	Consecuencia principal
Corte de energía	Interrupción de los servicios, pérdida de datos y apagado inesperado de equipos.
Sobretensión	Daños en componentes electrónicos sensibles debido a un aumento repentino de la tensión.
Subtensión	Funcionamiento inestable, reinicios y errores en equipos electrónicos.
Sobrecarga	Sobrecalentamiento de conductores y riesgo de incendio.
Cortocircuito	Elevada circulación de corriente que puede provocar daños materiales e incendios.
Descargas atmosféricas	Sobretensiones producidas por rayos que afectan instalaciones y equipos electrónicos.

Cada uno de estos riesgos puede afectar directamente la disponibilidad de los servicios informáticos, por lo que resulta necesario implementar medidas de protección adecuadas.

2.7.4. Puesta a tierra

La **puesta a tierra** es un sistema de protección que conecta determinados elementos metálicos de una instalación eléctrica con el terreno mediante un conductor especialmente diseñado para este fin. Su principal función consiste en derivar hacia la tierra las corrientes eléctricas producidas por una falla, evitando que circulen a través de las personas o de los equipos.

Gracias a este sistema es posible reducir significativamente el riesgo de descargas eléctricas y proteger los equipos electrónicos frente a determinadas fallas.

En una instalación informática, la puesta a tierra protege, por ejemplo:

- Gabinetes de computadoras;
- Servidores;
- Racks de comunicaciones;
- Tableros eléctricos;
- Equipos de red.

Una instalación sin una correcta puesta a tierra incrementa el riesgo de accidentes personales y puede favorecer daños en equipos sensibles.

2.7.5. Interruptores automáticos

Los **interruptores automáticos** son dispositivos de protección que interrumpen automáticamente el suministro eléctrico cuando detectan una condición anormal en un circuito.

Su objetivo es proteger las instalaciones eléctricas, los equipos y las personas frente a diferentes tipos de fallas.

Entre los dispositivos de protección más utilizados se encuentran la **llave térmica** y el **disyuntor diferencial**, que cumplen funciones diferentes y complementarias.

2.7.5.1. Llave térmica (Interruptor termomagnético)

La **llave térmica**, también conocida como **interruptor termomagnético**, protege la instalación eléctrica frente a **sobrecargas** y **cortocircuitos**.

Su nombre proviene de los dos mecanismos internos que utiliza para detectar fallas:

- **Protección térmica:** actúa cuando circula una corriente superior a la normal durante un cierto tiempo, como ocurre en una sobrecarga. Reacciona cuando se conectan muchos aparatos a la vez o se supera los amperios permitidos.
- **Protección magnética:** actúa de forma casi instantánea cuando detecta una corriente muy elevada, característica de un cortocircuito.

Cuando se produce cualquiera de estas situaciones, la llave térmica abre automáticamente el circuito e interrumpe el suministro eléctrico, evitando el sobrecalentamiento de los conductores y reduciendo el riesgo de incendios o daños en los equipos.

¿Cuándo actúa?

- Cuando se conectan demasiados equipos en un mismo circuito (sobrecarga).
- Cuando ocurre un cortocircuito.

- Cuando la corriente supera el valor nominal para el que fue diseñada.

¿Qué protege?

Principalmente protege:

- Los conductores eléctricos;
- La instalación eléctrica;
- Los equipos conectados.

Es importante destacar que **la llave térmica no protege directamente a las personas contra descargas eléctricas**.

2.7.5.2. Disyuntor diferencial (Interruptor diferencial)

El **disyuntor diferencial** es un dispositivo diseñado para proteger a las personas frente al riesgo de electrocución. Su funcionamiento se basa en comparar la corriente que ingresa al circuito con la corriente que regresa.

En condiciones normales ambas corrientes son iguales.

Si parte de la corriente se desvía por un camino no previsto —por ejemplo, a través del cuerpo de una persona debido a una falla de aislamiento— el disyuntor detecta esa diferencia e interrumpe inmediatamente el suministro eléctrico.

¿Cuándo actúa?

El disyuntor diferencial actúa cuando detecta una **corriente de fuga a tierra** superior al valor para el cual fue calibrado.

En instalaciones domiciliarias y comerciales es habitual encontrar dispositivos de **30 miliamperios (30 mA)**, ya que este valor ofrece una adecuada protección para las personas.

Su tiempo de actuación es muy breve, generalmente del orden de **milisegundos**, lo que reduce considerablemente el riesgo de lesiones graves por contacto eléctrico.

¿Qué protege?

El disyuntor diferencial protege principalmente:

- A las personas frente a contactos eléctricos indirectos;
- Frente a fugas de corriente ocasionadas por fallas de aislamiento;
- Frente a determinados riesgos de incendio provocados por corrientes de fuga.

No está diseñado para proteger contra sobrecargas ni cortocircuitos. Por este motivo siempre debe utilizarse junto con una llave térmica.

2.7.5.3. Diferencias entre la llave térmica y el disyuntor diferencial

Aunque ambos dispositivos suelen instalarse uno junto al otro en los tableros eléctricos, cumplen funciones distintas.

Dispositivo	Protege contra	Protege principalmente
Llave térmica (interruptor termomagnético)	Sobrecargas y cortocircuitos	Instalación eléctrica y equipos
Disyuntor diferencial	Corrientes de fuga a tierra	Personas y, en algunos casos, la instalación

En consecuencia, ambos dispositivos son complementarios y forman parte de un sistema de protección eléctrica integral.

2.7.6. Sistemas de Alimentación de Respaldo

Los sistemas de respaldo más utilizados son las **UPS (Uninterruptible Power Supply o Sistema de Alimentación Ininterrumpida)** y los **generadores eléctricos**. Ambos son complementarios y permiten garantizar la continuidad del suministro eléctrico cuando se produce una falla en la red.

2.7.6.1. UPS (Sistema de Alimentación Ininterrumpida)

Una **UPS** es un dispositivo que suministra energía eléctrica de manera inmediata cuando se interrumpe el suministro proveniente de la red.

Su funcionamiento se basa en baterías internas que almacenan energía y la entregan automáticamente a los equipos conectados cuando ocurre un corte eléctrico. La transición entre la red eléctrica y la batería es prácticamente instantánea, por lo que los equipos continúan funcionando sin interrupciones.

Las UPS se utilizan principalmente para proteger equipos sensibles, tales como:

- Servidores;
- Computadoras;
- Switches y routers;
- Sistemas de almacenamiento;
- Equipos de telecomunicaciones.

Además de mantener el suministro durante un corte de energía, muchas UPS incorporan funciones de regulación de tensión y protección frente a pequeñas variaciones del suministro eléctrico.

No obstante, su autonomía es limitada y depende de la capacidad de sus baterías y de la carga conectada. Generalmente permiten mantener los equipos funcionando durante algunos minutos, tiempo suficiente para guardar la información, apagar los sistemas de forma segura o esperar el arranque de un generador eléctrico.

2.7.6.2. Generadores eléctricos

Los **generadores eléctricos** son equipos que producen energía eléctrica utilizando un motor accionado, generalmente, por combustible diésel, gas natural o nafta.

A diferencia de una UPS, un generador no comienza a suministrar energía de forma instantánea. Después de un corte del suministro necesita algunos segundos para arrancar y estabilizar su funcionamiento. Una vez en servicio, puede alimentar la instalación durante un período prolongado, siempre que disponga de combustible y reciba el mantenimiento adecuado.

Los generadores son ampliamente utilizados en:

- Hospitales;
- Centros de cómputos;
- Bancos;
- Industrias;
- Aeropuertos;
- Organismos públicos;
- Empresas de telecomunicaciones.

En estas organizaciones resulta fundamental mantener operativos los servicios incluso durante cortes prolongados del suministro eléctrico.

2.7.7. Relación entre la UPS y el generador eléctrico

Aunque ambos dispositivos proporcionan energía de respaldo, cumplen funciones diferentes y complementarias.

Cuando ocurre un corte de energía, la **UPS** entra en funcionamiento de manera inmediata utilizando la energía almacenada en sus baterías, evitando que los equipos se apaguen.

Mientras tanto, el **generador eléctrico** inicia su proceso de arranque. Una vez que alcanza condiciones normales de funcionamiento, comienza a suministrar energía a la instalación y la UPS deja de utilizar sus baterías.

De esta manera:

- La **UPS** cubre los primeros segundos o minutos posteriores al corte;
- El **generador** mantiene el suministro durante cortes prolongados.

Esta combinación permite garantizar la continuidad del servicio y minimizar las interrupciones en los sistemas informáticos.

2.7.8. Cuadro resumen de los dispositivos estudiados

Dispositivo	¿Qué detecta?	¿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	Personas
Protector contra sobretensiones	Aumento de tensión	Equipos electrónicos
UPS	Corte de energía	Continuidad del servicio
Generador eléctrico	Corte prolongado de energía	Continuidad operativa

2.8. Protección Ambiental

2.8.1. Concepto

La **protección ambiental** comprende el conjunto de medidas destinadas a controlar las condiciones del entorno físico donde funcionan los equipos informáticos, con el fin de garantizar su correcto funcionamiento y prolongar su vida útil.

Factores como la temperatura, la humedad, el polvo o la presencia de agua pueden afectar el desempeño de computadoras, servidores, dispositivos de red y otros equipos tecnológicos, provocando fallas, interrupciones del servicio o daños permanentes.

Por este motivo, mantener condiciones ambientales adecuadas constituye un aspecto importante de la Seguridad Física.

2.8.2. Principales riesgos ambientales

Los equipos informáticos pueden verse afectados por diversos factores del ambiente.

Los más importantes son:

2.8.2.1. Temperaturas elevadas

El exceso de temperatura reduce el rendimiento de los equipos y acelera el desgaste de sus componentes electrónicos. En casos extremos puede provocar apagados automáticos, fallas de hardware o interrupciones del servicio.

2.8.2.2. Humedad

La humedad excesiva favorece la corrosión de los componentes electrónicos y aumenta el riesgo de cortocircuitos. Por el contrario, ambientes demasiado secos favorecen la acumulación de electricidad estática, que también puede dañar equipos sensibles.

2.8.2.3. Polvo

La acumulación de polvo dificulta la ventilación de los equipos, obstruye filtros y ventiladores, favorece el sobrecalentamiento y reduce la vida útil de los componentes.

2.8.2.4. Agua e inundaciones

Las filtraciones de agua, pérdidas en cañerías o inundaciones representan un riesgo importante para los equipos informáticos. Además del daño físico sobre los dispositivos, pueden producir cortocircuitos y pérdidas de información.

2.8.2.5. Vibraciones

Las vibraciones continuas pueden afectar equipos de almacenamiento, servidores y otros dispositivos delicados, especialmente en instalaciones industriales.

2.9. Centros de Datos

2.9.1. Concepto

Un **Centro de Datos (Data center o Centro de cómputos)** es una instalación especialmente diseñada para alojar y proteger la infraestructura tecnológica de una organización. En él se concentran los equipos responsables del almacenamiento, procesamiento y transmisión de la información, como servidores, dispositivos de red y sistemas de almacenamiento.

A diferencia de una oficina convencional, un centro de datos dispone de condiciones ambientales controladas, suministro eléctrico confiable y diversas medidas de Seguridad Física para garantizar el funcionamiento continuo de los sistemas informáticos.

Los centros de datos pueden pertenecer a una empresa, a un organismo público o ser operados por proveedores de servicios en la nube.

Su importancia radica en que constituyen el núcleo de los servicios tecnológicos de la organización. Una interrupción en su funcionamiento puede afectar aplicaciones, bases de datos, servicios web, correo electrónico y otros sistemas críticos.

2.9.2. Componentes principales de un Centro de Datos

Un centro de datos está formado por diversos elementos que trabajan de manera integrada para garantizar la disponibilidad de la infraestructura informática.

Entre los principales componentes se encuentran:

- Servidores;
- Sistemas de almacenamiento;

- Equipos de comunicaciones;
- Racks o gabinetes;
- Cableado estructurado;
- Sistemas de alimentación eléctrica;
- Sistemas de climatización;
- Sistemas de detección y extinción de incendios;
- Sistemas de control de acceso;
- Sistemas de videovigilancia.

Cada uno de estos componentes cumple una función específica y contribuye a mantener la continuidad de los servicios.

2.9.2.1. Servidores

Los servidores proporcionan los servicios informáticos de la organización, como aplicaciones, bases de datos, archivos o correo electrónico. Debido a su importancia, suelen instalarse en racks y contar con mecanismos de redundancia para minimizar el riesgo de interrupciones.

2.9.2.2. Equipos de comunicaciones

Incluyen switches, routers, firewalls y otros dispositivos que permiten la comunicación entre los distintos sistemas y el acceso a redes internas o externas. Una falla en estos equipos puede impedir el acceso a los servicios alojados en el centro de datos.

2.9.2.3. Sistemas de almacenamiento

Son los dispositivos donde se conserva la información de la organización. Dependiendo de las necesidades, pueden emplearse discos locales, cabinas de almacenamiento o sistemas de almacenamiento en red. La disponibilidad y confiabilidad de estos sistemas resulta fundamental para evitar pérdidas de información.

2.9.2.4. Racks

Los **racks** son estructuras metálicas diseñadas para alojar de forma ordenada los servidores y demás equipos informáticos.

Su utilización facilita:

- La organización del cableado;
- La ventilación de los equipos;
- El mantenimiento;
- La ampliación de la infraestructura.

Además, muchos racks disponen de cerraduras para restringir el acceso físico a los equipos.

2.9.3. Medidas de Seguridad Física en un Centro de Datos

Los centros de datos requieren un nivel de protección superior al de otras áreas de la organización, ya que alojan activos críticos para el funcionamiento de los sistemas de información.

Entre las principales medidas de Seguridad Física se destacan las siguientes.

2.9.3.1. Control de acceso físico

El acceso al centro de datos debe limitarse únicamente al personal autorizado. Para ello pueden emplearse distintos mecanismos, como:

- Tarjetas de proximidad;
- Sistemas biométricos;
- Cerraduras electrónicas;
- Registros de ingreso;
- Autenticación de múltiples factores.

El objetivo es impedir el acceso de personas no autorizadas y mantener un registro de quién ingresa y en qué momento.

2.9.3.2. Videovigilancia

Las cámaras de seguridad permiten supervisar permanentemente el interior y el exterior del centro de datos.

Las grabaciones pueden utilizarse para:

- Detectar incidentes;
- Verificar procedimientos;
- Apoyar investigaciones posteriores;
- Disuadir accesos no autorizados.

2.9.3.3. Protección contra incendios

Los centros de datos deben disponer de sistemas de detección temprana y de extinción adecuados para equipos electrónicos.

Es habitual utilizar:

- Detectores automáticos de humo;
- Alarmas;
- Agentes limpios para extinción;
- Extintores de dióxido de carbono (co_2).

Estos sistemas permiten minimizar los daños sobre la infraestructura informática.

2.9.3.4. Protección eléctrica

El funcionamiento continuo de un centro de datos depende de un suministro eléctrico estable y confiable.

Por ello es habitual contar con:

- Puesta a tierra;
- Protectores contra sobretensiones;
- Llaves térmicas;
- Disyuntores diferenciales;
- Ups;
- Generadores eléctricos.

Estas medidas reducen el riesgo de interrupciones provocadas por fallas eléctricas.

2.9.3.5. Control ambiental

Para garantizar el correcto funcionamiento de los equipos, el ambiente debe mantenerse dentro de parámetros adecuados.

Entre los aspectos que normalmente se controlan se encuentran:

- Temperatura;
- Humedad;
- Circulación del aire;
- Presencia de polvo;
- Filtraciones de agua.

En muchos centros de datos estos parámetros son supervisados mediante sensores automáticos.