FACULTAD DE CIENCIAS CONTABLES, AUDITORÍA
SISTEMAS DE CONTROL DE GESTIÓN Y FINANZAS
UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO

# INVESTIGACIÓN FORMATIVA (EXPOSICIÓN)

ICCAF

II-2025

# EXPO

## CIENCIA FACULTATIVA XV

**NOMBRE DEL TEMA:** SEGURIDAD FÍSICA Y LÓGICA, ENCRIPTACIÓN

**NÚMERO DE GRUPO:** _____ **TURNO DE PRESENTACIÓN:** _____

**DOCENTE GUÍA:** MARIO GERARDO PINTO VIRHUEZ

**INTEGRANTES:**

| | |
|---|---|
| ELIANA ROBLES ROSSEL | 222057432 |
| CARLOS JAIME HEREDIA CAYO | 221178020 |
| ANA VICTORIA FIGUEROA FLORES | 221010270 |
| DORIAN GUALBERTO RAMOS VILLAFAN | 221013828 |

NÚMERO INTERNO DE GRUPO:

APOYAN:

UAGRM

## INDICE

**UNIVERSIDAD / FACULTAD DE CIENCIAS CONTABLES, AUDITORÍA, SISTEMA DE CONTROL Y GESTIÓN Y FINANZAS**

# SEGURIDAD LOGICA Y FISICA, ENCRIPTACIÓN

## INTRODUCCIÓN

En la actualidad, los sistemas informáticos constituyen el núcleo operativo de casi todas las organizaciones modernas. Estos sistemas son esenciales para la continuidad de los procesos empresariales, académicos, administrativos y de comunicación; sin embargo, también son vulnerables a múltiples amenazas que pueden comprometer la integridad, disponibilidad y confidencialidad de los datos. En este contexto, la seguridad informática emerge como un conjunto de estrategias y mecanismos destinados a proteger los recursos tecnológicos frente a incidentes intencionales o accidentales.

Dentro de la seguridad informática, se destacan tres componentes fundamentales: la seguridad física, la seguridad lógica y la encriptación, los cuales actúan de manera complementaria para garantizar la protección integral de los sistemas. La seguridad física se refiere al conjunto de medidas preventivas, detectivas y correctivas orientadas a resguardar los componentes tangibles de un sistema informático, como servidores, computadoras, dispositivos de red y centros de datos, frente a amenazas ambientales, robos, sabotajes o desastres naturales. Sin una infraestructura física adecuada, incluso las soluciones tecnológicas más avanzadas se vuelven ineficaces.

Por su parte, la seguridad lógica comprende los métodos y herramientas que protegen los recursos digitales —software, datos y redes— frente a accesos no autorizados o ataques informáticos. Incluye políticas de control de acceso, autenticación de usuarios, uso de firewalls, sistemas antivirus, detección de intrusos, gestión de parches y auditorías. Su objetivo principal es garantizar que solo los usuarios y procesos legítimos puedan acceder y modificar la información, manteniendo su integridad y confidencialidad.

Finalmente, la encriptación o cifrado representa uno de los pilares más robustos de la seguridad lógica. Es una técnica basada en algoritmos matemáticos que transforma la información legible en un formato ininteligible para quienes no poseen la clave adecuada. Existen distintos tipos de cifrado —simétrico, asimétrico y de hash que se aplican en comunicaciones seguras, almacenamiento de contraseñas, transmisión de

datos en redes y protección de bases de datos. La encriptación garantiza que, incluso si los datos son interceptados, no puedan ser interpretados por terceros no autorizados.

En conjunto, la seguridad física, lógica y la encriptación forman un sistema integral que protege los sistemas informáticos frente a una amplia gama de amenazas. Su implementación adecuada no solo preserva los activos tecnológicos y la información crítica, sino que también fortalece la confianza, la eficiencia operativa y la resiliencia ante incidentes. Este informe desarrolla cada uno de estos componentes de manera detallada, destacando sus principios, tipos, herramientas y ejemplos aplicados en entornos informáticos modernos.

**JUSTIFICACIÓN**

La creciente dependencia de las organizaciones hacia la tecnología y los sistemas informáticos ha generado una necesidad ineludible de garantizar la seguridad de la información. En la actualidad, tanto entidades públicas como privadas administran grandes volúmenes de datos sensibles —financieros, personales, académicos o estratégicos— que, de ser comprometidos, podrían provocar graves consecuencias operativas, económicas y legales. Ante este escenario, la seguridad física, la seguridad lógica y la encriptación se convierten en componentes esenciales para la protección integral de los recursos tecnológicos.

La seguridad física constituye la primera línea de defensa dentro de cualquier infraestructura informática, pues protege los elementos tangibles que hacen posible el funcionamiento de los sistemas, como servidores, equipos de red, dispositivos de almacenamiento y centros de datos. Sin medidas adecuadas de control de acceso, vigilancia, protección eléctrica o detección de incendios, los equipos pueden ser vulnerables a robos, sabotajes, fallas eléctricas o desastres naturales. Garantizar la seguridad física permite mantener la disponibilidad de los servicios y minimizar el impacto de eventos imprevistos que afecten la continuidad operativa.

Por otro lado, la seguridad lógica abarca las políticas, protocolos y herramientas que protegen los componentes intangibles del sistema —software, redes y datos— frente a amenazas como virus, malware, ataques cibernéticos o accesos no autorizados. Esta dimensión de la seguridad se centra en salvaguardar la confidencialidad, integridad y disponibilidad de la información mediante mecanismos como la autenticación de usuarios, firewalls, antivirus, sistemas de detección y prevención de intrusos, así como

controles de acceso basados en roles. La correcta aplicación de estas medidas reduce significativamente la superficie de ataque y fortalece la ciberresiliencia institucional.

La encriptación, por su parte, complementa de forma estratégica las anteriores medidas al proteger directamente los datos, transformándolos en información ilegible para quienes no poseen las claves correctas. Su aplicación es esencial en la transmisión de información a través de redes públicas, el almacenamiento de contraseñas, la comunicación entre servidores y clientes, y la protección de bases de datos. De esta forma, incluso si los mecanismos físicos o lógicos llegaran a fallar, la encriptación actúa como una última barrera de seguridad, impidiendo el acceso o la manipulación indebida de la información.

El estudio conjunto de estos tres pilares permite comprender que la seguridad informática no depende de un único componente, sino de la integración coordinada de medidas físicas, lógicas y criptográficas. Este enfoque integral contribuye al desarrollo de infraestructuras informáticas seguras, resilientes y confiables, alineadas con estándares internacionales como ISO/IEC 27001 o los lineamientos del NIST Cybersecurity Framework.

Por tanto, este trabajo se justifica en la necesidad de analizar y comprender de forma técnica los mecanismos, tipos y herramientas de seguridad aplicables en los sistemas informáticos modernos. El conocimiento de estos elementos permitirá a los futuros profesionales en informática implementar estrategias efectivas de protección, anticipar riesgos, reducir vulnerabilidades y promover entornos tecnológicos seguros que respalden el funcionamiento y la confianza en las instituciones digitales.

## OBJETIVO GENERAL

Analizar de manera integral los mecanismos, tipos y herramientas de seguridad física, seguridad lógica y encriptación aplicados en los sistemas informáticos, con el propósito de identificar estrategias efectivas que garanticen la protección de la infraestructura tecnológica, la integridad de los datos y la continuidad operativa frente a amenazas internas y externas.

## OBJETIVOS ESPECÍFICOS

- **En el ámbito de la Seguridad Física**
  1. Identificar los principales riesgos físicos que pueden afectar la infraestructura de los sistemas de información, tales como incendios, robos, sabotajes o fallas eléctricas.
  2. Analizar la importancia del control de acceso físico mediante el uso de cerraduras electrónicas, tarjetas de proximidad y sistemas biométricos en la protección de centros de datos.
  3. Evaluar las condiciones ambientales (temperatura, humedad, energía eléctrica) que influyen en el funcionamiento óptimo y seguro de los equipos informáticos.

- **En el ámbito de la Seguridad Lógica**
  1. Analizar las políticas y procedimientos de control de acceso que regulan la autenticación y autorización de usuarios dentro de un entorno informático.
  2. Examinar la importancia de las actualizaciones, parches de seguridad y copias de respaldo en la mitigación de vulnerabilidades del sistema.
  3. Describir los tipos de seguridad lógica (de software, red, sistema operativo, base de datos y aplicaciones) aplicables a la protección de los sistemas de información.
- **En el ámbito de la Encriptación**
  1. Explicar los conceptos fundamentales de la encriptación y su importancia dentro de la seguridad informática.
  2. Distinguir los tipos de cifrado (simétrico, asimétrico, híbrido y hashing), sus características, ventajas y desventajas.
  3. Ejemplificar la aplicación práctica de la encriptación en sistemas informáticos, como en el cifrado de discos, bases de datos, comunicaciones y almacenamiento en la nube.

## DESARROLLO DEL TEMA

### SEGURIDAD INFORMÁTICA

Se entiende por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad,

confidencialidad, y buen uso de la información que reside en un sistema de información. Desde este enfoque veremos la seguridad física y lógica.

## SEGURIDAD FÍSICA

Cuando hablamos de seguridad física nos referimos a todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina. Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

Consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos e información confidencial se aplica tanto a equipos de hogar y pequeñas oficinas como a servidores y cpds. La seguridad física está enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

**Las principales amenazas son**:

- Ocasionadas por el hombre: Como robos, destrucción de la información o de equipos, fraude y sabotaje.
- Desastres naturales: Alteraciones y cortes del suministro eléctrico, (incendios, tormentas e inundaciones).
- Disturbios y sabotajes internos o externos.

## PRINCIPIOS

### Controles de accesos

El software es muy fácilmente sustraible y las cintas y discos son fáciles de copiar sin dejar ni rastro. El control de acceso no solo requiere la capacidad de identificación sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo de área o de sector dentro de una empresa. Quien se encarga de controlar esto es el servicio de vigilancia de la empresa, quien se encarga de pedir las credenciales de identificación.

### Sistemas biométricos

Es una tecnología que realiza mediciones de forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación

consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Ejemplos:

- Huellas digitales.
- Reconocimiento de voz.
- Ojos.
- Manos. Etc...

**Beneficios:**

- Elimina la necesidad de tener una tarjeta para acceder y de una contraseña difícil de recordar que alguien puede ver en un papel.

**Protección electrónica**

Se llama así a la detección de robo, asalto de incendios mediante la utilización de sensores conectados a centrales de alarmas.

- **Ejemplo 1 - Barreras infrarrojas y de microondas:** Transmiten y recibe haces de luces infrarrojas y de microondas. Cuando el haz es interrumpido se activa el sistema de alarma.

- **Ejemplo 2 - Detector ultrasónico:** Éste equipo utiliza ultrasonidos para crear un campo de ondas, cualquier movimiento que realice un cuerpo dentro del espacio protegido creará una perturbación del campo que activará la alarma.

- **Ejemplo 3 - Circuitos cerrados de televisión(CCTV):** Son monitores y cámaras situados en los lugares estratégicos y accesos.

**Condiciones ambientales**

Normalmente se reciben por privado los avisos de tormentas, tifones y catástrofes sísmicas, Las condiciones atmosféricas severas se asocian a ciertas partes del mundo del mundo la probabilidad de que ocurran está documentada.

Incendios: Es el enemigo número 1 de las computadoras ya que puede destruir fácilmente archivos y programas. Factores a contemplar para reducir los riesgos de incendios:

- Mantener los ordenadores limpios por dentro para evitar cortocircuitos.

- Mantener la instalación eléctrica.

- Deben instalarse equipos anti-incendio manuales y automáticos.

- No debemos estar cerca de zonas con materiales inflamables, explosivos.
- inundaciones: dejar la instalación eléctrica en alto y acondicionar puertas para contener el agua.

**PROTECCIÓN FÍSICA DE EQUIPO**

**instalaciones**

Las características de una instalación con varios equipos deben tener:

- Instalación eléctrica adecuada: por ejemplo, los enchufes deben contar con tomas de tierra y la corriente suministrada debe ser lo más estable posible para evitar cortes de tensión.
- Por otra parte, debemos de realizar mantenimiento del suministro eléctrico, es conveniente instalar SAI's para evitar las anomalías de la corriente eléctrica.
- Control de acceso: Hay que controlar quien entra al ordenador o a la sala.
- Protección frente a incendios: Tenemos sistemas de prevención como, por ejemplo: Detectores de humo y alarmas, orden y limpieza.

**SAI's**

Sistemas de alimentación ininterrumpida: Problemas de energía. El 50% de los problemas en los equipos y en la perdida de información son debidos a interrupciones y perturbaciones en el suministro de la red eléctrica.

El papel del SAI es suministrar energía en caso de fallo de suministro en un intervalo de tiempo corto. Los 9 problemas de la energía son:

Apagones, Micro-cortes, Alto voltaje momentáneo, Bajadas de tensión sostenida, Subidas de tensión, Ruido eléctrico, Cambio en las frecuencias, Micro-picos, Distorsión armónica misma red de los equipos, como, por ejemplo, fotocopiadoras, fax, etc...

SAI: Un SAI es un dispositivo cuya finalidad es proporcionar u suministro eléctrico a los equipos conectados a él cuándo se produce un corte en la corriente eléctrica.

**CENTRO DE PROCESADO DE DATOS**

Esos sistemas que centralizan bases de datos, servicios de email, gestión de usuarios, etc.… necesitan unas instalaciones físicas y unos requerimientos de hardware que reciben el nombre de CPD (Centro de Proceso de Datos). Los sistemas informáticos a

esta escala requieren servidores con varios procesadores y unidades de disco, sistemas de comunicaciones avanzados (varios routers, switches, etc.…), equipos de alimentación redundantes, dispositivos de copia de seguridad, etc... Estos equipos deben de trabajar a una temperatura ambiente baja (entre 17 y 19Cº).

**sistema de seguridad del CPD**

La sala o edificio dedicado al CPD debe contar con las siguientes medidas de seguridad frente a riesgos:

- Sistemas contra incendios: Debemos de tener material ignífugo en las salas además de detectores, extintores, mangueras, etc.
- Sistemas eléctricos: La instalación debe ser óptima para la carga estimada que va a soportar contando con la previsión de futuro por si hay ampliación. El diseño de las canalizaciones es fundamental para aislar los cables y también para evitar caídas o accidentes.

**centros de respaldo**

A pesar de todas las medidas de seguridad anteriores siempre puede ocurrir alguna catástrofe y perder todos los datos del CPD, para ello de manera adicional se crean centros o salas de respaldo, que son replicas más o menos exactas del CPD diseñadas para que si falla puedan tomar el control.

La primera medida es separarlos físicamente (entre 20 y 40km) teniendo en cuenta que las salas no deben ser idénticas, tenemos varias tipologías de centros de respaldo:

- **Sala fría:** CPD externo con toda la infraestructura necesaria para, en caso de contingencia, trasladar todos los servidores y equipos, y reinstalar el sistema a partir de copias de seguridad, se puede tardar una semana, pero es lo más barato.
- **Sala caliente:** Es un CPD análogo principal de modo que, en caso de contingencia, solo hay que restaurar los datos del último momento.
- **Mutual Backup:** Se llega a un acuerdo con otra organización para hacer un backup mutuo entre sí, cada organización reserva un espacio de su CPD para los servidores de respaldo de la otra que pueden estar apagados o encendidos.

- **Mirror Site o Centro Espejo:** Es una evolución de la sala caliente en la que los datos son replicados en tiempo real de un CPD a otro, para lo cual se necesitan redes de alta velocidad y fiables.

**Tipos de Seguridad Física**

**1. Control de Acceso Físico**

- Sistema que restringe el ingreso a instalaciones o áreas críticas, asegurando que solo el personal autorizado acceda a servidores o laboratorios.
  **Funcionamiento:** uso de puertas y torniquetes, tarjetas de proximidad, códigos PIN, huella dactilar o reconocimiento facial, con registro automático de entradas según niveles de autorización.
  **Aplicación:** centros de datos, oficinas de TI, bancos o universidades.
  **Ejemplos:** lectores biométricos ZKTeco y tarjetas HID.
  **Ventajas:** evita accesos indebidos, permite auditoría de ingresos y reduce riesgos internos.

**2. Vigilancia y Monitoreo**

- Consiste en la supervisión continua de las instalaciones mediante cámaras, sensores y personal de seguridad.
  **Funcionamiento:** uso de CCTV, alarmas, sensores de movimiento y análisis inteligente de video.
  **Aplicación:** en perímetros, almacenes y zonas donde se manejan datos o equipos de alto valor.
  **Ejemplos:** cámaras Hikvision, Dahua o monitoreo centralizado en hospitales.
  **Ventajas:** previene robos y sabotajes, permite respuesta rápida y facilita investigaciones.

**3. Protección de Equipos y Dispositivos**

- Conjunto de medidas para evitar el robo o daño de equipos informáticos y de red.
  **Funcionamiento:** anclajes, racks cerrados, sellos de seguridad y bloqueo de puertos USB.
  **Aplicación:** oficinas, laboratorios y centros de datos.
  **Ejemplos:** candados Kensington y racks cerrados para servidores.

**Ventajas:** protege activos valiosos, disuade robos y mantiene la integridad de los dispositivos.

**4. Protección contra Incendios**

- Sistemas para detectar y extinguir incendios antes de causar daños graves.
  **Funcionamiento:** detectores de humo o calor, alarmas automáticas, sistemas de gas inerte, extintores y planes de evacuación.
  **Aplicación:** salas de servidores, oficinas y almacenes con riesgo eléctrico.
  **Ejemplos:** sistemas FM-200 o Novec 1230, detectores Honeywell y extintores $CO_2$.
  **Ventajas:** reduce pérdidas, protege al personal y garantiza respuesta inmediata ante emergencias.

**5. Protección contra Desastres Ambientales**

- Medidas que previenen daños por inundaciones, cortes eléctricos o condiciones extremas.
  **Funcionamiento:** UPS y generadores de respaldo, sensores de temperatura y humedad, climatización de precisión y elevación de equipos.
  **Aplicación:** centros de datos y oficinas críticas, especialmente en zonas con riesgo ambiental.
  **Ejemplos:** UPS APC, aire acondicionado de precisión y sensores Monnit.
  **Ventajas:** mantiene la operación durante emergencias y protege los equipos de factores ambientales.

**SEGURIDAD LOGICA**

La seguridad lógica se refiere a los controles específicos establecidos para administrar el acceso a los sistemas informáticos y los espacios físicos dentro del centro de datos. Usar una puerta cerrada para salvaguardar la entrada de la sala de servidores del centro de datos puede ser una mejor práctica de seguridad física, pero tener que participar en la autenticación de dos factores para abrir la puerta es una forma de seguridad lógica.

La seguridad lógica ayuda a proteger contra amenazas conocidas como ataques cibernéticos, pero también protege a los centros de datos de sí mismos. El error humano es una de las causas más frecuentes de tiempo de inactividad y otras desgracias de TI, ya sea por negligencia o intención maliciosa.

Mediante la implementación de protocolos lógicos de seguridad y la actualización continua de las listas de acceso de usuarios, las compañías pueden garantizar que nadie pueda acceder a sus datos valiosos sin su autorizaci

## CARACTERÍSTICAS DE LA SEGURIDAD LÓGICA

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo

## PRINCIPALES BRECHAS EN LA SEGURIDAD LOGICA INFORMATICA

Las amenazas lógicas afectan al software, datos o redes sin dañar el hardware. Entre ellas destacan los virus, ataques DoS, phishing y troyanos, que pueden propagarse por dispositivos externos y comprometer sistemas completos, robando información o paralizando operaciones.

### Malware

- El *malware* (software malicioso) incluye virus, spyware, gusanos, troyanos o rootkits, diseñados para infiltrarse y dañar equipos sin autorización del usuario. Su presencia puede alterar archivos, espiar información o inutilizar sistemas.

### Programas No Testeados

- Instalar software no verificado representa un riesgo, pues puede contener errores de programación o vulnerabilidades (como *buffer overflows*) que permitan a atacantes obtener privilegios, acceder a archivos protegidos o modificar datos del sistema.

### Errores Humanos y del Operador

- Los fallos cometidos por usuarios u operadores son una causa frecuente de incidentes de seguridad. La falta de capacitación o descuido en el manejo de información puede comprometer la integridad de los datos, por lo que se requiere concienciación y cumplimiento de protocolos.

### Mal Uso de la Tecnología

- El uso inadecuado de dispositivos o redes corporativas, como acceder a sitios inseguros o conectar memorias personales, puede introducir malware en los sistemas y afectar gravemente la información empresarial.

- **Fraudes**

- Tanto los fraudes internos como externos pueden perjudicar gravemente a una organización. Entre los más comunes están los fraudes con tarjetas de crédito, cheques, proveedores falsos, robo de identidad o estafas por telemercadeo. La vigilancia constante y los controles financieros reducen su impacto.

- **Accesos No Autorizados**

- El acceso indebido, ya sea interno o externo, constituye una de las mayores amenazas. Para prevenirlo, se aplican múltiples capas de seguridad como cortafuegos, protección de red, cifrado de datos y monitoreo de usuarios, evitando así violaciones de información sensible.

- **Amenazas de Ingeniería Social**

- Estas explotan el factor humano mediante manipulación psicológica. Técnicas como *phishing*, *spear phishing*, *smishing*, *vishing*, *pretexting* o *tailgating* buscan obtener datos confidenciales o acceso no autorizado. La prevención se basa en la capacitación continua, pruebas de simulación y políticas estrictas de verificación de identidad.

## ¿POR QUÉ ES TAN IMPORTANTE LA SEGURIDAD LÓGICA PARA LAS EMPRESAS?

A pesar de la preocupación por los ataques cibernéticos y los desastres naturales, la verdad es que la mayoría del tiempo de inactividad del servidor es causada por un error humano. La seguridad lógica no solo reduce la posibilidad de errores humanos al limitar el acceso, sino que también hace que sea más fácil rastrear errores y diagnosticar problemas cuando ocurren.

Al rastrear qué tipo de errores ocurrieron y documentar quién los cometió, las organizaciones pueden apuntalar vulnerabilidades y educar a los usuarios para ayudarlos a evitar errores similares en el futuro.

### Tipos de Seguridad Lógica

### 1. Control de Acceso

Es la primera barrera de defensa, encargada de identificar, autenticar y autorizar a los usuarios antes de permitirles acceder a recursos del sistema.
**Funcionamiento:** identificación (usuario o biometría), autenticación (contraseña o PIN), autorización (asignación de permisos) y registro de accesos para auditoría.
**Ejemplos:** Active Directory, sistemas biométricos en bancos y Okta/Auth0 para aplicaciones en la nube.
**Ventajas:** protege datos, permite auditorías y reduce fraudes internos.

**2. Seguridad en Redes**

Protege las comunicaciones entre equipos y servidores frente a interceptaciones o ataques externos.
**Funcionamiento:** uso de firewalls, sistemas IDS/IPS, VPNs y segmentación de redes.
**Ejemplos:** VPN en bancos, firewalls Fortinet en hospitales y detección de tráfico anómalo con Snort.
**Ventajas:** evita ciberataques, protege los datos en tránsito y limita daños en caso de intrusión.

**3. Seguridad en Software y Sistemas Operativos**

Garantiza que los sistemas estén actualizados y libres de vulnerabilidades.
**Funcionamiento:** aplicación de parches, antivirus, listas blancas de programas y soluciones de protección de endpoints.
**Ejemplos:** Windows Defender + Intune en empresas, Deep Freeze en escuelas.
**Ventajas:** previene malware, mantiene la estabilidad del sistema y evita instalaciones no autorizadas.

**4. Seguridad en Bases de Datos**

Protege la información crítica de accesos o modificaciones indebidas.
**Funcionamiento:** gestión de roles, cifrado de datos, auditorías y enmascaramiento de información.
**Ejemplos:** Oracle Database Vault y SQL Server TDE.
**Ventajas:** resguarda datos sensibles, cumple normas de privacidad y reduce riesgos de filtración.

**5. Copias de Seguridad (Backups)**

Permiten recuperar datos perdidos o dañados, siendo una defensa esencial ante ataques o fallos.
**Funcionamiento:** copias automáticas periódicas, almacenamiento en diferentes

ubicaciones y pruebas de restauración.
**Ejemplos:** backups cifrados en bancos o respaldo académico en la nube.
**Ventajas:** minimiza pérdidas, acelera la recuperación y protege contra ransomware.

**6. Registro y Monitoreo de Actividades**

Supervisa acciones dentro de los sistemas para detectar incidentes a tiempo.
**Funcionamiento:** herramientas SIEM que recopilan y analizan registros, generando alertas ante comportamientos sospechosos.
**Ejemplos:** Splunk, ELK Stack, IBM QRadar y el visor de eventos de Windows.
**Ventajas:** permite detección temprana, rastreo de actividades y apoyo en auditorías.

**7. Seguridad Criptográfica**

Asegura la confidencialidad e integridad de los datos mediante cifrado y autenticación digital.
**Funcionamiento:** uso de algoritmos AES o RSA, firmas y certificados digitales (HTTPS).
**Ejemplos:** plataformas bancarias con TLS/SSL, cifrado de discos con BitLocker y correos protegidos con PGP.
**Ventajas:** impide lectura no autorizada, evita alteraciones y garantiza identidad del emisor.

**Gestión de Incidentes y Continuidad de Negocio**

La gestión de incidentes de seguridad consiste en establecer un conjunto de procedimientos y protocolos que permitan detectar, analizar, responder y mitigar los efectos de cualquier evento que ponga en riesgo la seguridad de la información o la infraestructura tecnológica. Una correcta gestión no solo minimiza el impacto del incidente, sino que también permite aprender de él para evitar su repetición.

Un aspecto clave dentro de esta gestión es el Plan de Recuperación ante Desastres (DRP, Disaster Recovery Plan), el cual define cómo se deben restaurar los sistemas críticos en caso de fallos graves como incendios, inundaciones, fallos eléctricos o ciberataques masivos. Este plan se complementa con el Plan de Continuidad de Negocio (BCP, Business Continuity Plan), que asegura que la organización pueda seguir operando, aunque sea de manera limitada, mientras se recupera por completo de la contingencia.

Ejemplo: en un ataque de ransomware, una empresa puede perder acceso a todos sus servidores y bases de datos. Si dispone de un DRP con copias de seguridad cifradas y almacenadas en un centro de respaldo, podrá restaurar sus operaciones en cuestión de horas o días, evitando pérdidas millonarias y daños a su reputación.

## ENCRIPTACIÓN

### Definición de Encriptación

La palabra encriptación es una mezcla de inglés y griego que significa “ocultar”. La encriptación de datos es el proceso de esconder información de participantes maliciosos o alguien que esté mirando. A este proceso también se le puede conocer como encriptación informática.

Encriptamos datos para mantenerlos confidenciales. La encriptación de datos es parte de un tipo más amplio de tácticas defensivas de ciberseguridad conocidas como “Seguridad de datos”. La seguridad de datos se trata de mantener nuestros datos a salvo de accesos no autorizados, bloqueos por ransomware (que es una forma maliciosa de encriptación) brechas o corrupción maliciosa (por ejemplo, cambiar datos para volverlo inservible), etcétera.

### ¿Qué es la encriptación de datos?

La encriptación de datos es el proceso mediante el cual la información se transforma en un formato ilegible para cualquiera que no tenga la clave de descifrado adecuada. Este proceso es esencial en la protección de información sensible contra accesos no autorizados y ataques cibernéticos.

Básicamente es una técnica de cifrado que convierte datos en texto codificado (conocido como ciphertext), haciendo que la información original sea ininteligible sin el conocimiento específico para revertir la transformación (la clave de descifrado). Esta técnica asegura que solo las personas autorizadas puedan acceder y leer los datos en su forma original.

### Principales objetivos de la encriptación

Confidencialidad: Protege la información de ser accesada por personas no autorizadas.

Integridad: Asegura que los datos no han sido alterados durante la transmisión o el almacenamiento.

Autenticidad: Verifica que los datos provienen de una fuente confiable y no han sido manipulados.

No repudio: Previene que una parte niegue haber realizado una acción o transmisión de datos.

**Cómo funciona la encriptación de datos**

Uno de los métodos más efectivos para proteger la información es la encriptación de datos. Este proceso garantiza que los datos sensibles permanezcan inaccesibles para usuarios no autorizados, protegiéndolos contra ciberataques y accesos no deseados.

**Generación de Claves:** El primer paso en el proceso de encriptación de datos es la generación de claves criptográficas. Estas claves pueden ser simétricas (una sola clave para encriptar y desencriptar) o asimétricas (una clave pública para encriptar y una clave privada para desencriptar).

**Algoritmo de Encriptación:** Se selecciona un algoritmo de encriptación, como AES (Advanced Encryption Standard) para encriptación simétrica, o RSA (Rivest-Shamir-Adleman) para encriptación asimétrica. Estos algoritmos aplican complejas operaciones matemáticas a los datos y la clave, produciendo el texto cifrado.

**Proceso de Encriptación:** Los datos originales se combinan con la clave mediante el algoritmo seleccionado, convirtiéndose en texto cifrado. Este texto cifrado no tiene sentido sin la clave correspondiente.

**Transmispión y Almacenamiento Seguro:** El texto cifrado se transmite o almacena en sistemas de almacenamiento seguro. Si un atacante intercepta los datos en esta etapa, no podrá leerlos sin la clave de desencriptación.

**Desencriptación:** Cuando el destinatario autorizado recibe los datos cifrados, utiliza la clave correspondiente para revertir el proceso de encriptación, devolviendo el texto cifrado a su forma original.

**Tipos de Encriptación de Datos**

**Encriptación Simétrica:** Utiliza una sola clave para encriptar y desencriptar los datos. Es rápida y eficiente para grandes volúmenes de datos, pero la distribución segura de la clave puede ser un desafío.

El cifrado simétrico es un tipo de cifrado en el que se utiliza la misma clave para cifrar y descifrar los datos. Este método ha sido fundamental en criptografía durante décadas y se valora especialmente por su velocidad y eficacia. Cuando hay que cifrar rápidamente grandes cantidades de datos, el cifrado simétrico suele ser la opción preferida.

Algunos algoritmos populares de encriptación simétrica son:

AES (Estándar de Cifrado Avanzado): Conocido por su alta seguridad y velocidad, el AES se utiliza ampliamente en aplicaciones gubernamentales, militares y comerciales.

DES (Estándar de Cifrado de Datos): Aunque fue sustituido en gran medida por AES debido a su menor seguridad, DES sentó las bases de muchos sistemas de encriptación.

Blowfish: Un método de encriptación rápido y compacto que se utiliza a menudo en aplicaciones de software en las que la alta velocidad es fundamental.

Estos algoritmos se eligen en función del nivel de seguridad requerido y de la potencia de procesamiento disponible.

Cómo funciona la encriptación simétrica

En el cifrado simétrico, se utiliza una sola clave para proteger los datos. He aquí un desglose básico del proceso:

Texto plano: El dato o mensaje original que hay que cifrar.

Cifrado: El texto plano se cifra utilizando una sola clave, lo que da como resultado el texto cifrado (un formato ilegible).

Descifrar: La misma clave se utiliza para volver a convertir el texto cifrado en texto plano legible.

Por ejemplo, imagina dos personas, Alicia y Bob, que quieren comunicarse de forma segura. Si Alice quiere enviar un mensaje a Bob, lo encripta con una clave compartida. Bob puede entonces descifrar el mensaje utilizando la misma clave, asegurándose de que sólo ellos pueden leer el mensaje


Ventajas de la encriptación simétrica

Velocidad y eficacia: Como el cifrado simétrico requiere menos pasos computacionales, suele ser más rápido y eficiente que otros métodos, por lo que es ideal para grandes volúmenes de datos.

Fuerte protección de datos a gran escala: Los robustos algoritmos utilizados en el cifrado simétrico son excelentes para proteger datos a escala.

Menor coste computacional: Como utiliza una sola clave y menos pasos de procesamiento, tiene un coste menor en términos de recursos del sistema.

**Inconvenientes de la encriptación simétrica**

Problema de la distribución de claves: Ambas partes deben tener la misma clave, que puede ser difícil de compartir de forma segura en redes abiertas. Si la clave es interceptada durante la transmisión, los datos se vuelven vulnerables.

Escalabilidad limitada: A medida que aumenta el número de usuarios, la gestión de claves se convierte en un reto. Cada par de usuarios necesita una clave única, lo que puede ser difícil de gestionar en organizaciones grandes.

Estos inconvenientes hacen que el cifrado simétrico sea menos ideal en situaciones en las que el intercambio seguro de claves es difícil o cuando se requiere escalar entre muchos usuarios.

**Encriptación Asimétrica:** A diferencia de la encriptación simétrica, la encriptación de clave asimétrica utiliza una clave pública y una clave privada para encriptar y

desencriptar datos. Este método elimina la necesidad de compartir la misma clave, ya que una clave (la pública) se utiliza para cifrar, y la otra (la privada) para descifrar.

Emplea un par de claves, una pública y otra privada. La clave pública se utiliza para encriptar los datos, mientras que la clave privada se usa para desencriptarlos. Esto facilita el intercambio seguro de datos, aunque es más lento que la encriptación simétrica.

El cifrado asimétrico, también conocido como criptografía de clave pública, se utiliza habitualmente para comunicaciones seguras en línea, firmas digitales y protocolos SSL/TLS para establecer conexiones seguras entre navegadores web y servidores.

Algunos algoritmos de encriptación asimétrica muy utilizados son:

RSA (Rivest-Shamir-Adleman): RSA es uno de los sistemas de encriptación de clave pública más comunes, conocido por su seguridad y versatilidad.

ECC (Criptografía de Curva Elíptica): La ECC proporciona alta seguridad con longitudes de clave más cortas, lo que la hace más rápida y eficaz para los dispositivos móviles.

DSA (Algoritmo de Firma Digital): Utilizado principalmente para firmas digitales, el DSA garantiza la autenticidad e integridad de los datos.

Cada algoritmo ofrece ventajas únicas y se elige en función de las necesidades específicas de seguridad del sistema.

Cómo funciona la encriptación asimétrica

El proceso de encriptación asimétrica implica dos claves que trabajan juntas para asegurar los datos:

Clave pública: Se utiliza para encriptar los datos. Esta clave se comparte abiertamente y cualquiera puede utilizarla para encriptar información.

Clave privada: Se utiliza para desencriptar los datos. Esta clave permanece secreta y sólo la conoce el destinatario.

Por ejemplo, supongamos que Alicia quiere enviar un mensaje seguro a Bob. Ella cifra su mensaje utilizando la clave pública de Bob. Cuando Bob recibe el mensaje cifrado,

utiliza su clave privada para descifrarlo. Aunque se intercepte el mensaje cifrado, sólo Bob puede leerlo, ya que es el único que tiene la clave privada.

**Ventajas de la encriptación asimétrica**

Escalabilidad: Una única clave pública puede compartirse con varios usuarios, lo que hace que el cifrado asimétrico sea más escalable en redes grandes.

Intercambio de claves simplificado: Sólo es necesario compartir abiertamente la clave pública, eliminando la necesidad de una distribución segura de claves.

Mayor seguridad en redes abiertas: Sólo la clave privada del destinatario puede descifrar los datos, lo que los hace seguros, aunque la clave pública esté ampliamente disponible.

Capacidad de firma digital: El cifrado asimétrico permite las firmas digitales, que confirman la identidad del remitente y la integridad de los datos.

Estas ventajas hacen que el cifrado asimétrico sea una opción excelente para la comunicación segura a través de redes públicas y para verificar la autenticidad de los datos.

**Desventajas de la encriptación asimétrica**

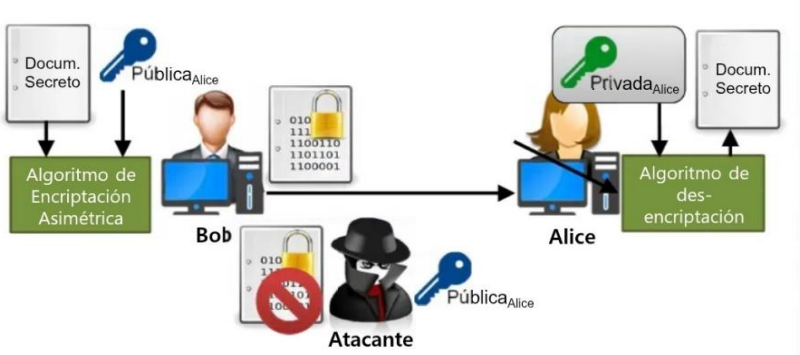
Complejidad: Implementar el cifrado asimétrico puede ser más complicado, sobre todo con la gestión segura de la clave privada.

Exigencias computacionales: El cifrado asimétrico es más lento y requiere más potencia de cálculo que el cifrado simétrico.

Bajo rendimiento para grandes conjuntos de datos: Debido a su complejidad, suele ser poco práctico para encriptar archivos grandes.

Mayores tamaños de clave: Requiere tamaños de clave más grandes que el cifrado simétrico para una seguridad comparable, lo que aumenta las exigencias de procesamiento.

Estos inconvenientes hacen que el cifrado asimétrico sea menos adecuado para cifrar datos almacenados en masa, aunque destaca en el intercambio seguro de claves y la verificación digital.




Diferencias entre el cifrado simétrico y el cifrado asimétrico

| simétrico | Cifrado asimétrico |
|---|---|
| **Usa una sola clave para cifrar y descifrar datos** | Usa una clave pública para cifrar los datos, y una clave privada para descifrar la información |
| **Proceso de cifrado más rápido** | Proceso de cifrado más lento |
| **Los tamaños de clave de ejemplo son de 128 o 256 bits** | Los tamaños de clave de ejemplo son de 2048 bits o mayores |
| **No utiliza muchos recursos** | Utiliza más recursos |
| **El texto cifrado es más pequeño o del mismo tamaño que el texto simple original.** | El texto cifrado es más grande o del mismo tamaño que el texto cifrado original |
| **Tanto los algoritmos simétricos como los asimétricos proporcionan capacidad de autenticación** | Tanto los algoritmos simétricos como los asimétricos proporcionan capacidad de autenticación. Solo el no repudio se puede lograr con un algoritmo asimétrico. |
| **Los algoritmos de ejemplo son AES, DES, 3DES, IDEA y Blowfish.** | Los algoritmos de ejemplo son los algoritmos RSA, ECC, DSA y El Gamal. |
| **Mejor en el manejo y transferencia de grandes cantidades de datos** | Mejor en el manejo y transferencia de cantidades más pequeñas de datos |
| **Existe el riesgo de que alguien robe la llave si no se gestiona adecuadamente** | Tiene el riesgo de perder la clave privada (el par de claves es irrevocable) |

**Importancia de la encriptación de datos**

Protección contra el Acceso No Autorizado: La encriptación asegura que solo las personas autorizadas puedan acceder a la información sensible, protegiéndola de hackers y usuarios malintencionados.

Confidencialidad: Al encriptar datos, se garantiza que la información permanezca confidencial, incluso si es interceptada durante su transmisión.

Integridad de Datos: La encriptación ayuda a mantener la integridad de los datos, asegurando que no sean alterados durante su transmisión o almacenamiento.

Cumplimiento Normativo: Muchas regulaciones, como el GDPR (Reglamento General de Protección de Datos) y la HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud), requieren el uso de encriptación para proteger los datos sensibles.

**¿Qué pasa cuando la encriptación de datos falla?**

La encriptación de datos es una técnica fundamental para proteger información confidencial frente a accesos no autorizados. Su funcionamiento se basa en el uso de llaves criptográficas, que son cadenas de números o caracteres empleadas para codificar y decodificar los datos. Generalmente, estas llaves se utilizan en pares: una para quien envía la información y otra para quien la recibe.

A pesar de su eficacia, la encriptación no es completamente infalible. Los atacantes pueden intentar vulnerarla mediante un proceso llamado ataque de fuerza bruta, que consiste en adivinar la llave probando todas las combinaciones posibles. La dificultad de este ataque depende de la longitud de la llave: las más cortas son más fáciles de descifrar, mientras que las más largas ofrecen una mayor seguridad.

En la actualidad, las llaves de 128 bits son el estándar, ya que poseen una cantidad casi infinita de combinaciones posibles, lo que hace prácticamente imposible romper la encriptación. Sin embargo, aunque la probabilidad sea mínima, siempre existe un margen de riesgo de que la protección falle.

**Soluciones de encriptación de datos**

Existen dos tipos básicos de soluciones de encriptación: las que encriptan tus datos inmóviles, y las que encriptan tus datos en tránsito.

**Encriptación de datos inmóviles**

Esta corresponde a tus archivos guardados. En este caso, es preciso configurar cualquier aplicación que necesite acceso a datos encriptados con los medios para desencriptarlos.

**Encriptación de datos en tránsito**

Esta tiene que ver con tus comunicaciones. Aquí se hace necesario que tanto el emisor como el receptor tengan capacidades de cifrado y descifrado. Estos requerimientos crean problemas administrativos, y la situación se puede volver compleja al enviar datos encriptados fuera de tu organización.

Los hackers pueden ir por ambas: por ejemplo, tus archivos guardados (datos inmóviles) o tus comunicaciones (datos en tránsito). Respecto a dichas comunicaciones, mencionar que pueden ser tanto correos electrónicos como mensajes internos, sistema a sistema y a través de redes que manejan datos en nuestras organizaciones.

**¿Quién necesita usar la encriptación de datos?**

La respuesta es simple: casi todos nosotros. No tienes que ser un agente secreto para querer mantener tus datos confidenciales. De hecho, es muy probable que estés usando encriptación de datos incluso sin saberlo. Muchos servicios tecnológicos cifran y descifran tus datos de manera de mantenerlos a salvo hasta que se utilizan. Los negocios deberían encriptar datos que pudieran hacer daño a sus resultados financieros de existir una brecha. Los individuos de a pie deberían encriptar información sensible, como el historial médico o el número identificador nacional (RUT, DNI, etc.

**Algoritmo de encriptación**

Un algoritmo de encriptación es el método utilizado para transformar los datos en texto encriptado. Es decir, un algoritmo de encriptación hace referencia al conjunto de instrucciones matemáticas y lógicas que se utilizan para transformar información legible en un formato ilegible, protegiendo la confidencialidad y seguridad durante su transmisión o almacenamiento.

Los algoritmos de encriptación utilizan técnicas matemáticas para mezclar los datos y convertirlos en un código que sólo puede ser descifrado con la clave de encriptación correcta.

**Algoritmos De Cifrado**

**Cifrado Triple DES**

El Triple DES se diseñó para reemplazar al algoritmo Data Encryption Standard (o DES; En español: “estándar para cifrado de datos”), el cual los hackers aprendieron a descifrar muy pronto. En una época, el Triple DES fue el estándar recomendado y el algoritmo simétrico más ampliamente utilizado en el sector.

El Triple DES utiliza tres claves individuales de 56 bits cada una. La longitud total de la clave llega a los 168 bits, pero los expertos afirman que lo más probable es que la fuerza de la clave sea equivalente a los 112 bits.

**Cifrado RSA**

El RSA es un algoritmo de cifrado de clave pública y el estándar para el cifrado de datos que se envían por internet. También es uno de los métodos que se emplean en los programas PGP y GPG.

A diferencia del Triple DES, el RSA se considera un algoritmo de cifrado asimétrico porque utiliza un par de claves. Se usa la clave pública para cifrar el mensaje y una clave privada para descifrarlo. A los atacantes les tomaría una cantidad considerable tanto de tiempo como de poder de cómputo lograr descifrar este código de cifrado.

**Advanced Encryption Standards (AES)**

El Advanced Encryption Standard (o AES; en español: “estándar de encriptación avanzado”) es un algoritmo considerado como fiable por el gobierno de los EE. UU. y muchas otras organizaciones, y se le utiliza como estándar.

Si bien es extremadamente eficiente en su forma de 128 bits, el cifrado AES también utiliza claves de 192 y de 256 bits para cifrado de alto rendimiento.

Al AES se le considera capaz de resistir cualquier ataque, exceptuando ataques de fuerza bruta, que procuran descifrar los mensajes utilizando todas las combinaciones posibles en la cifra de 128, 192 o 256 bits. Sin embargo, los expertos en seguridad opinan que el AES se convertirá eventualmente en el estándar de cifrado de datos en el sector privado.

Estándar de encriptación de datos triple (3DES): es un algoritmo de encriptación simétrico por bloques, que emplea bloques de 64 bits para cifrar la información. Además de ello, realiza 3 rondas de encriptación para elevar un nivel más la seguridad del mensaje original.

**aplicaciones de software y seguridad en la web.**

Criptografía de curva elíptica (ECC): consiste en un método de encriptado asimétrico que se basa en las curvas elípticas sobre campos infinitos. Es considerado como un método avanzado para la encriptación de la información y garantiza una amplia seguridad a las claves de encriptación que son de muchos caracteres.

**Desventajas de la encriptación de datos**

Ransomware: es posible que los ciber atacantes utilicen el cifrado con malas intenciones. Esto ocurre cuando los hackers logran acceder a información, la encriptan y luego exigen recompensa para liberar la información.

Existen tres formas relevantes de aplicar la encriptación para ayudar a la privacidad del usuario: encriptación en tránsito, encriptación en reposo y encriptación de extremo a extremo:

La encriptación en tránsito. Se refiere a la protección de los datos mientras están siendo transmitidos entre dos puntos, como por ejemplo entre un navegador y un servidor web, o entre dos dispositivos móviles.

Este tipo de encriptación evita que terceros intercepten y accedan a la información durante su traslado. Se basa en protocolos como TLS (Transport Layer Security), VPN (Red Privada Virtual) o SSH (Secure Shell), y es ampliamente utilizada en servicios de mensajería, formularios web y transferencias de archivos.

Su función es comparable a enviar una carta dentro de un sobre sellado: aunque alguien intercepte el sobre, no podrá leer el contenido sin romperlo.

**Buenas Prácticas para el Cifrado de Comunicaciones y Datos en Reposo**

El cifrado es una herramienta fundamental para proteger la confidencialidad e integridad de la información tanto en tránsito como en reposo. Su aplicación correcta permite evitar accesos no autorizados y garantizar la autenticidad de las comunicaciones.

Una de las principales buenas prácticas es el uso de protocolos TLS/SSL para las comunicaciones web seguras. Estos protocolos aseguran que los datos transmitidos entre clientes y servidores estén cifrados, evitando que terceros intercepten información

sensible. Es esencial que todos los sitios y servicios que manejen datos personales o financieros utilicen HTTPS con certificados válidos.

Asimismo, la autenticación de comunicaciones es vital para verificar la identidad de las partes involucradas. Esto impide que los datos sean manipulados o interceptados por agentes no autorizados. Un ejemplo común es el uso de certificados digitales en redes VPN corporativas, donde tanto el usuario como el servidor deben autenticarse mutuamente.

En cuanto a la encriptación de datos en reposo, su propósito es proteger la información cuando se encuentra almacenada y no en tránsito, ya sea en discos duros, bases de datos, dispositivos móviles o servicios en la nube. Se recomienda utilizar algoritmos robustos como AES-256, así como herramientas de cifrado como BitLocker o FileVault, que garantizan que los datos permanezcan inaccesibles incluso si alguien obtiene acceso físico o digital a los dispositivos.

Finalmente, el cifrado de extremo a extremo (E2EE) refuerza la privacidad en las comunicaciones digitales al asegurar que solo el emisor y el receptor puedan acceder al contenido del mensaje. Este método emplea criptografía asimétrica mediante el uso de claves públicas y privadas, de modo que ni siquiera el proveedor del servicio pueda descifrar los datos.

En conjunto, estas prácticas —TLS/SSL, autenticación, encriptación en reposo y cifrado de extremo a extremo— constituyen la base de una estrategia sólida de seguridad informática orientada a la protección integral de la información.

## CONCLUSIONES

El análisis de la seguridad física, la seguridad lógica y la encriptación en los sistemas informáticos demuestra que la protección de la información y la infraestructura tecnológica debe abordarse de manera integral y complementaria. Ningún mecanismo de seguridad es suficiente por sí solo; la combinación de medidas físicas, controles lógicos y técnicas criptográficas permite crear entornos informáticos más resilientes frente a amenazas tanto internas como externas.

La seguridad física constituye la base sobre la cual se sustentan las demás capas de protección. Sin un entorno físico seguro —protegido ante incendios, fallas eléctricas, accesos indebidos o desastres naturales—, los sistemas informáticos quedan expuestos a interrupciones que pueden ocasionar pérdidas económicas o de información irreversibles. La correcta aplicación de controles de acceso, videovigilancia, climatización, respaldo energético y planes de contingencia garantiza la disponibilidad y continuidad de los servicios.

Por su parte, la seguridad lógica representa la defensa activa del entorno digital. Mediante políticas de autenticación, monitoreo, segmentación de redes y actualización de software, se logra reducir la superficie de ataque y fortalecer la integridad de los sistemas. La implementación de tecnologías como firewalls, IDS/IPS, VPN y SIEM ha demostrado ser eficaz en la detección y mitigación temprana de amenazas cibernéticas.

La encriptación, finalmente, es el mecanismo que asegura la confidencialidad y autenticidad de los datos, incluso cuando estos son interceptados o sustraídos. Gracias a los algoritmos de cifrado modernos (AES, RSA, SHA, TLS), los sistemas informáticos pueden garantizar que la información se mantenga protegida tanto en tránsito como en reposo, convirtiéndose en una última barrera contra el acceso no autorizado.

En conjunto, estos tres componentes conforman un modelo integral de seguridad informática, donde la prevención, detección y respuesta operan de manera coordinada. Las organizaciones que aplican este enfoque alcanzan mayores niveles de ciberresiliencia, cumpliendo además con estándares internacionales como ISO/IEC 27001 y NIST CSF, los cuales promueven la gestión estructurada de la seguridad de la información.

**RECOMENDACIONES**

- Implementar políticas de seguridad integral que contemplen tanto los aspectos físicos como los lógicos, alineadas con estándares internacionales (ISO/IEC 27001, NIST).
- Establecer controles de acceso físico y lógico con autenticación multifactor y registros de auditoría para garantizar trazabilidad y responsabilidad en el manejo de información.

- Capacitar periódicamente al personal técnico y administrativo en buenas prácticas de ciberseguridad, gestión de contraseñas, manejo de información y respuesta ante incidentes.
- Mantener actualizado el software y hardware crítico de los sistemas, aplicando parches de seguridad y revisiones periódicas que reduzcan vulnerabilidades.
- Implementar sistemas de monitoreo continuo (SIEM) que permitan detectar patrones anómalos y reaccionar de forma oportuna ante ciberataques o fallas del sistema.
- Asegurar la infraestructura física mediante vigilancia, sensores ambientales, sistemas antiincendios y fuentes de energía ininterrumpida (UPS).
- Aplicar la encriptación de extremo a extremo para toda la información sensible, tanto en tránsito (protocolos HTTPS, VPN, TLS) como en reposo (bases de datos, respaldos, discos duros).
- Diseñar e implementar planes de contingencia y recuperación ante desastres, que incluyan respaldo de datos y simulacros regulares para evaluar la eficacia de las medidas.
- Realizar auditorías de seguridad internas y externas para identificar vulnerabilidades y medir el nivel de cumplimiento de las políticas de seguridad.
- Promover una cultura organizacional de seguridad informática, en la que todos los usuarios comprendan su papel en la protección de la información y los sistemas.

**BIBLIOGRAFIA**

1. **Avigilon**. (s.f.). *Seguridad física: Planificación, medidas y ejemplos*. Recuperado de: https://www.avigilon.com/es/blog/physical-security-guide
2. **Rittal**. (2023, 28 de septiembre). *Seguridad física en informática: Ejemplos y tipos en una infraestructura tecnológica*. Recuperado de: https://rittalnet.cl/seguridad-fisica/
3. **Segurilatam**. (2022, 1 de febrero). *Seguridad física para proteger dispositivos informáticos en el área de trabajo*. Recuperado de: https://www.segurilatam.com/actualidad/seguridad-fisica-para-proteger-dispositivos-informaticos-en-el-area-de-trabajo_20220201.html
4. **Dongee**. (2024, 26 de julio). *¿Qué es la Seguridad Física y Lógica en Informática?*. Recuperado de: https://www.dongee.com/tutoriales/que-es-la-seguridad-fisica-y-logica-en-informatica/
5. **Aratek**. (2024, 20 de noviembre). *Seguridad física 101: una guía completa*. Recuperado de: https://www.aratek.co/es/news/physical-security-101-a-comprehensive-guide
6. **IBM**. (s.f.). *¿Qué son los controles de seguridad?*. Recuperado de: https://www.ibm.com/mx-es/think/topics/security-controls
7. **Universidad de Valencia**. (s.f.). *Seguridad Física*. Recuperado de: https://www.uv.es/sto/cursos/icssu/html/ar01s04.html
8. **Inesem**. (2023, 27 de abril). *Tipos de amenazas físicas en seguridad informática*. Recuperado de: https://www.inesem.es/revistadigital/gestion-integrada/amenazas-seguridad-fisica-sistemas-de-informacion
9. https://kinsta.com/es/base-de-conocimiento/que-es-la-encriptacion/
10. https://www.kingston.com/latam/blog/data-security/what-is-encryption
11. https://web.dev/learn/privacy/encryption?hl=es-419

🌐 **Webgrafía**

**Fortinet**. (s.f.). *¿Qué es el control de acceso?*. Recuperado de: https://www.fortinet.com/lat/resources/cyberglossary/access-control

**SafetyCulture**. (2024, 11 de diciembre). *Seguridad física: La guía definitiva*. Recuperado de: https://safetyculture.com/es/temas/seguridad-fisica/

**Wikipedia**. (2025, 15 de septiembre). *Seguridad informática*. Recuperado de: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

**Wikipedia**. (2025, 15 de septiembre). *Ataque DMA*. Recuperado de: https://es.wikipedia.org/wiki/Ataque_DMA

**Wikipedia**. (2025, 15 de septiembre). *Endurecimiento (informática)*. Recuperado de:https://es.wikipedia.org/wiki/Endurecimiento_%28inform%C3%A1tica%29

**Wikipedia**. (2025, 15 de septiembre). *Zona desmilitarizada (informática)*. Recuperado de:https://es.wikipedia.org/wiki/Zona_desmilitarizada_%28inform%C3%A1tica%29

https://www.cloudflare.com/es-es/learning/ssl/what-is-encryption/

https://www.ibm.com/es-es/think/topics/cryptography-history

https://blog.mailfence.com/es/cifrado-simetrico-vs-asimetrico/