

Seguridad Informática - Teoría

Introducción

La **seguridad informática** es el conjunto de medidas, prácticas y tecnologías destinadas a proteger los **sistemas informáticos**, los **datos** y las **comunicaciones** frente a accesos no autorizados, daños o interrupciones.

Su objetivo principal es que los sistemas funcionen **de forma correcta, segura y disponible** para los usuarios autorizados.

Terminología Básica

Para comprender la seguridad informática es importante manejar ciertos conceptos fundamentales:

- **Activo**: recurso que debe protegerse (hardware, software, datos, personas, servicios...).
 - **Amenaza**: todo aquello que puede causar un daño a los activos (atacantes, virus, incendio, error humano...).
 - **Vulnerabilidad**: debilidad o fallo que puede ser explotado por una amenaza (un puerto abierto, una contraseña débil, un enchufe sin toma de tierra...).
 - **Riesgo**: probabilidad de que una amenaza aproveche una vulnerabilidad y cause un impacto.
 - **Impacto**: consecuencias de que un riesgo se materialice (pérdida económica, de datos, de reputación, interrupción de servicio...).
 - **Control / Medida de Seguridad**: acción o mecanismo que se aplica para reducir el riesgo (cifrado, cortafuegos, políticas de acceso, copias de seguridad...).
-

Amenazas y Agentes de Amenaza

- **Tipos de amenazas (según su origen)**:
 - **Naturales**: incendios, inundaciones, terremotos, tormentas eléctricas...
 - **Accidentales**: errores humanos (borrar un fichero sin querer), averías, cortes de luz...
 - **Intencionadas**: ataques de ciberdelincuentes, robo de equipos, malware, espionaje...
- **Agentes de amenaza (quién causa el daño)**:
 - **Externos**: atacantes en Internet, ladrones, competencia desleal...
 - **Internos**: empleados descontentos, usuarios descuidados, personal de limpieza...
 - **Factores ambientales**: fuego, humo, agua, polvo, animales, etc.

Es importante entender que **el error humano** es una de las causas más frecuentes de incidentes de seguridad.

Partes de un Sistema Informático / Tipos de Activos

Un sistema informático está compuesto por varios elementos que deben ser protegidos para garantizar su correcto funcionamiento y seguridad:

1. **Hardware**: componentes físicos del sistema (servidores, ordenadores, impresoras, dispositivos de red...).
2. **Software**: aplicaciones y sistemas operativos que gestionan el hardware y los datos.
3. **Datos / Información**: contenido que se procesa y almacena (bases de datos, documentos, correos...).
4. **Personas**: usuarios, administradores, técnicos... que interactúan con el sistema.

5. **Servicios:** servicios de red, páginas web, correo electrónico, aplicaciones en la nube, etc. Todos ellos son **activos** que pueden sufrir amenazas y deben ser protegidos.

Principios de la Seguridad Informática

Los principios de la seguridad informática establecen las bases para proteger la información y los sistemas. Los principales son:

Confidencialidad

Garantiza que solo las personas **autorizadas** puedan acceder a la información.

Ejemplos: - Cifrado de datos
- Contraseñas seguras
- Control de accesos (usuarios y permisos)

Integridad

Asegura que la información se mantenga **correcta y sin alteraciones no autorizadas**.

Ejemplos:

- Funciones hash
- Firmas digitales
- Sumas de verificación
- Control de versiones de archivos

Disponibilidad

Garantiza que la información y los recursos estén **disponibles cuando los usuarios autorizados los necesitan**.

Ejemplos:

- Redundancia de servidores
- Copias de seguridad
- Sistemas de alimentación ininterrumpida (SAI)
- Planes de recuperación ante desastres

Autenticación

Verifica la **identidad** de los usuarios o sistemas.

Ejemplos:

- Usuario y contraseña
- Autenticación multifactor (MFA)
- Certificados digitales, tarjetas inteligentes, tokens

No Repudio

Evita que un usuario pueda **negar haber realizado una acción** o enviado cierta información.

Ejemplos:

- Firmas digitales
 - Certificados electrónicos
 - Registros de auditoría (logs)
-

Políticas y Modelos de Seguridad

La seguridad informática se organiza desde lo más general (normas) a lo más concreto (mecanismos técnicos):

- **Política de seguridad**

Conjunto de normas y reglas que definen **qué se quiere proteger y cómo deben actuar los usuarios**.
> Ejemplo: “Los datos de clientes solo pueden ser consultados por personal de ventas autorizado”.

- **Modelo de seguridad**

Forma de traducir la política a una **estructura lógica** dentro del sistema.

> Ejemplo: Control de Acceso Basado en Roles (RBAC), donde el rol “ventas” tiene acceso a determinados datos.

- **Mecanismos o medidas de seguridad**

Herramientas concretas que hacen posible el modelo.

> Ejemplo: usuarios, contraseñas, permisos de ficheros, firewalls, cifrado, etc.

Tipos de Seguridad

Seguridad Lógica

Conjunto de medidas técnicas para proteger los **sistemas y datos digitales**.

Ejemplos:

- Contraseñas
- Cifrado
- Cortafuegos (firewalls)
- Antivirus y antimalware
- Sistemas de detección de intrusos (IDS)

Seguridad Física

Conjunto de medidas que protegen los **componentes físicos** del sistema informático.

Ejemplos:

- Cerraduras en puertas y armarios
- Cámaras de seguridad
- Control de acceso físico (tarjetas, llaves, huella)

- Ubicación segura de servidores y cableado
-

Seguridad Pasiva y Seguridad Activa

Seguridad Pasiva

Medidas destinadas a **prevenir** incidentes de seguridad o minimizar su impacto.
Normalmente **no reaccionan** en tiempo real, pero reducen daños.

Ejemplos:

- Copias de seguridad (backups)
- SAI (Sistemas de Alimentación Ininterrumpida)
- Diseño del CPD (sala de servidores)
- Políticas de seguridad
- Seguro de equipos

Seguridad Activa

Medidas que buscan **detectar y responder** a incidentes de seguridad **en tiempo real o casi real**.

Ejemplos:

- Firewalls
 - IDS/IPS (sistemas de detección y prevención de intrusos)
 - Monitorización de red
 - Antimalware en tiempo real
 - Alertas y sistemas de log
-

Proceso de Planificación de la Seguridad

Antes de aplicar medidas de seguridad, es fundamental realizar una **planificación**:

1. **Identificación de activos**
 - ¿Qué queremos proteger? (equipos, datos, servicios, personas...).
2. **Análisis de amenazas y vulnerabilidades**
 - ¿Qué les puede pasar? (robo, incendio, malware, fallos eléctricos...).
 - ¿Qué debilidades existen? (contraseñas débiles, falta de copias, enchufes sin tierra...).
3. **Evaluación de riesgos**
 - ¿Qué probabilidad hay de que ocurra el problema?
 - ¿Qué impacto tendría?
4. **Definición de controles**
 - Elegir medidas de seguridad para reducir los riesgos (técnicas, físicas, organizativas).
5. **Implementación**
 - Aplicar las medidas elegidas (configurar firewalls, hacer copias, comprar un SAI...).
6. **Monitorización y revisión**
 - Comprobar periódicamente si las medidas funcionan y actualizarlas cuando sea necesario.

Auditorías de Seguridad

Una **auditoría de seguridad** es un proceso de revisión y análisis de los sistemas de información para comprobar:

- Si se cumplen las políticas de seguridad.
- Si las medidas implantadas son adecuadas.
- Si existen vulnerabilidades o malas prácticas.

Tras la auditoría se elabora un **informe** con:

- Fallos encontrados
 - Nivel de riesgo
 - Recomendaciones de mejora
-

Protección Física de los Equipos

La protección física es la **primera línea de defensa**. Si un atacante puede entrar en la sala de servidores y llevarse un disco, da igual que esté todo cifrado y con contraseñas fuertes.

A continuación, se describen algunas amenazas físicas y medidas para reducir su impacto.

Incendios

Los incendios pueden destruir equipos e instalaciones.

Medidas:

- Detectores de humo y calor
- Extintores adecuados y visibles
- Sistemas de extinción que no dañen los equipos (por ejemplo, gases inertes en CPD)
- Revisiones periódicas de la instalación eléctrica

Humo

El humo puede dañar componentes internos, provocar corrosión y fallos de lectura/escritura.

Medidas:

- Mantener los equipos en áreas bien ventiladas
- No fumar cerca de los equipos
- Sistemas de filtrado de aire en salas críticas

Polvo

El polvo:

- Puede actuar como **conductor** y provocar cortocircuitos
- Puede ser un **aislante térmico** y causar sobrecalentamiento

Medidas:

- Filtros en las entradas de aire de equipos y armarios
- Filtros de aire en la sala
- Limpieza periódica de equipos y entorno

Explosiones

Riesgo extremo, relacionado con gases, combustibles, etc.

Medidas:

- Evitar almacenar materiales inflamables junto a equipos
- Cumplir las normas de seguridad del edificio y de prevención de riesgos laborales

Temperaturas Extremas

Temperaturas demasiado altas o bajas afectan al rendimiento y a la vida útil de los equipos.

Medidas:

- Mantener una temperatura ambiente adecuada en salas de servidores y oficinas
- Sistemas de climatización y ventilación
- Sensores de temperatura con alarmas

Elementos Biológicos

Insectos y roedores pueden anidar en equipos, morder cables y provocar cortocircuitos.

Medidas:

- Mantener las zonas limpias, sin comida ni basura
- Usar barreras físicas (rejillas, burletes...)
- Revisar periódicamente para detectar posibles plagas

Tormentas Eléctricas

Generan sobretensiones que pueden dañar los equipos, incluso apagados.

Medidas:

- Protectores contra sobretensiones
- Buen sistema de puesta a tierra
- Desconectar equipos en tormentas fuertes si es posible
- Uso de SAI para proteger frente a picos y cortes

Vibraciones

Las vibraciones, incluso suaves, pueden:

- Aflojar conexiones

- Desgastar componentes
- Afectar a discos duros mecánicos

Medidas:

- Colocar equipos en superficies estables y niveladas
- Utilizar soportes antivibración cuando sea necesario
- Evitar mover los equipos mientras están encendidos
- Asegurar correctamente los componentes internos

Agua y Humedad

El agua y la humedad alta pueden causar cortocircuitos y corrosión.

Medidas:

- No colocar equipos cerca de ventanas sin protección o tuberías
- Evitar tener equipos en el suelo (usar soportes o racks)
- Deshumidificadores en salas muy húmedas
- Revisar posibles fugas de agua

Robos

El robo de dispositivos puede provocar pérdida de datos y filtraciones de información.

Medidas:

- Cerrar con llave aulas, despachos y salas de servidores
 - Anclar equipos (cables de seguridad, anclajes a mesa, racks cerrados)
 - Control de acceso físico (tarjetas, llaves, códigos, biometría)
 - Cámaras de seguridad y sistemas de alarma
-

Medidas de Protección Física

Control de Acceso Físico

Conjunto de medidas para **controlar quién puede entrar** a ciertas zonas:

- Puertas con llave o tarjeta
- Torniquetes, porteros automáticos
- Registro de visitas
- Diferentes niveles de acceso (recepción, oficinas, CPD...)

Métodos de Autenticación Física

Se basan en los mismos principios que en lógica, pero aplicados al acceso físico:

- **Algo que tienes:** llaves, tarjeta magnética, tarjeta RFID
- **Algo que sabes:** código PIN para abrir una puerta
- **Algo que eres:** huella dactilar, reconocimiento facial

Métodos de Disuasión

Medidas que buscan que el atacante **se lo piense dos veces**:

- Carteles de “Zona videovigilada”
- Cámaras visibles
- Presencia de personal de seguridad
- Alarmas sonoras

Vigilancia Natural

Diseño del entorno para que haya “ojos” observando:

- Pasillos y entradas visibles desde la recepción
- Cristales en puertas de salas importantes
- Evitar rincones ocultos en zonas sensibles

Iluminación de Seguridad

La iluminación adecuada reduce riesgos de robo y vandalismo:

- Luz suficiente en accesos y salidas
- Iluminación en aparcamientos y alrededores
- Luces de emergencia

Sistemas de Detección de Intrusos

Detectan intentos de acceso no autorizado:

- Sensores de movimiento
- Sensores de apertura de puertas y ventanas
- Alarmas conectadas a central o a policía

Sistemas de Alimentación Ininterrumpida (SAI)

Un **SAI** (Sistema de Alimentación Ininterrumpida, en inglés UPS) es un dispositivo que:

- Proporciona **energía eléctrica durante un tiempo limitado** cuando hay un corte de luz.
- Filtra y estabiliza la corriente, protegiendo de picos y bajadas de tensión.

Esto permite: - Mantener encendidos servidores y equipos críticos el tiempo suficiente para **guardar el trabajo y apagarlos correctamente**.

- Evitar daños por apagados bruscos o por sobretensiones.

Tipos básicos de SAI (explicados de forma sencilla)

- **Off-line**
 - El más sencillo y barato.
 - Solo entra en funcionamiento cuando se va la luz.
 - Adecuado para **puestos de trabajo individuales**.
 - **Line-Interactive**
 - Mejora el off-line regulando mejor la tensión.
 - Ideal para oficinas con cortes y variaciones de tensión frecuentes.
 - **On-line (doble conversión)**
 - La protección más alta.
 - La carga siempre se alimenta desde el SAI, no directamente de la red.
 - Usado en **servidores y CPD**.
-

Amenazas Lógicas o de Software

Además de los peligros físicos, los sistemas informáticos también pueden sufrir **amenazas lógicas**, es decir, ataques o problemas que afectan al **software y a los datos**.

Malware (Software Malicioso)

Programa diseñado para dañar o aprovecharse de un sistema.

- **Virus**: se “pega” a archivos y se ejecuta cuando abrimos dichos archivos.
- **Gusanos (worms)**: se propagan solos por la red sin intervención del usuario.
- **Troyanos**: programas que aparentan ser algo útil o inofensivo, pero esconden código malicioso.
- **Ransomware**: cifra los archivos y pide un “rescate” (dinero) para recuperarlos.

Medidas básicas: - Tener antivirus actualizado. - No instalar programas de origen desconocido. - No abrir adjuntos sospechosos.

Ingeniería Social

Ataques que se centran en **engaños a las personas** para que ellas mismas revelen información o hagan algo peligroso.

- **Phishing**: correos o mensajes falsos que imitan a bancos, empresas o servicios para robar contraseñas o datos.
- **Suplantación de identidad**: alguien se hace pasar por técnico, jefe, compañero, etc. para conseguir acceso.

Medidas básicas:

- Desconfiar de correos que piden contraseñas o datos personales.
- Comprobar siempre la dirección web (URL).
- No dar datos sensibles por teléfono o email sin verificar quién está al otro lado.

Errores de Configuración y Uso

A veces los problemas no vienen de un “hacker”, sino de una **mala configuración** o un **mal uso**:

- Contraseñas débiles o repetidas.
- Redes Wi-Fi sin contraseña o con cifrado inseguro.
- Compartir carpetas a “Todos” sin control.
- No instalar actualizaciones de seguridad.

Medidas básicas:

- Usar contraseñas fuertes.
 - Configurar bien la red y los permisos de archivos.
 - Mantener el sistema y los programas actualizados.
-