# Seguridad Informática - 2º SMR
# Tema 1: Conceptos básicos de Seguridad Informática

## 1.1. Razones para la seguridad informática

Tanto en las empresas como en los domicilios particulares el uso de sistemas informáticos con acceso a Internet es generalizado por lo que preservar la información y la integridad de estos sistemas es primordial.

Hoy en día realizamos muchas gestiones a través de Internet, negocios, compras, interacción con el banco... todas estas gestiones son de carácter bastante privado y delicado por lo que hay que mantener nuestro sistema lo más seguro posible para evitar que se intercepten nuestros datos o que se infecte la red de nuestra casa o empresa.

Cualquier fallo podría suponer una gran pérdida económica o en el peor de los casos podríamos sufrir suplantación de nuestra personalidad para realizar delitos.

> **Ejercicios propuestos**
>
> **1.1.1.** Busca en Internet tres noticia sobre vulneración de la seguridad de algún sistema informático.

## 1.2. Objetivos de la seguridad informática

Los objetivos principales de la seguridad informática son proteger los **activos** informáticos:

- **La información contenida:** Uno de los elementos más importantes del sistema. Se debe evitar que usuarios externos o no autorizados puedan acceder a ella y que los usuarios autorizados puedan acceder en cualquier momento.
- **La infraestructura física:** Se debe velar porque los equipos funcionen de la forma adecuada previendo medidas en caso de robo, incendio, accidentes o desastres naturales...
- **Los usuarios:** Se deben establecer unas normas que minimicen los riesgos por parte de usuarios no autorizados como: perfiles de usuario, horarios de funcionamiento, restricción de acceso a ciertos lugares, planes de emergencia...

Según la ISO27002 “La seguridad de la información se puede caracterizar por la preservación de la confidencialidad, integridad y la disponibilidad”.

Según INFOSEC Glosssary 2000: “ Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican”.

### 1.2.1. Confidencialidad

La confidencialidad intenta prevenir la divulgación de información a personas o sistemas no autorizados. De esta manera un documento será confidencial si sólo puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada.

### 1.2.2 Integridad

Propiedad que busca mantener los datos libres de modificaciones no autorizadas.

### 1.2.3 Disponibilidad

Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella en todo momento.

### 1.2.4 Autenticación

Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento refleja. En los sistema informáticos la autenticación normalmente se realiza mediante un usuario y contraseña.

### 1.2.5 No repudio

Que la comunicación entre emisor y receptor queden garantizadas y que ninguno pueda negar que ha existido comunicación.

- **No repudio en origen:** El emisor no puede negar la comunicación ya que se le envían pruebas al receptor de tal comunicación.
- **No repudio en destino:** El receptor no puede negar la comunicación porque el emisor tiene pruebas de la recepción.

Si la autenticidad prueba quien es el autor de un documento y cuál es el destinatario, el no repudio prueba que es el mismo autor quien envía la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

# 1.3 Mecanismos de seguridad

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad , la integridad y la disponibilidad de un sistema informático.

Se pueden clasificar según su función en:

- **Preventivos:** Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
- **Detectivos:** Actúan también antes de que un hecho ocurra pero su función es revelar la presencia de agentes no detectados en algún elemento del sistema.
- **Correctivos:** Actúan después de que haya ocurrido el hecho y su función es corregir las consecuencias.

Ejemplos de mecanismos:

### 1.3.1 Mecanismos software o lógicos

Cortafuegos, antivirus, antispam, utilización de números de serie, protección anticopia, encriptación de la información, uso de contraseñas, formación de usuarios del sistema.

### 1.3.2 Mecanismos hardware o físicos

SAI, extintores, cámaras de seguridad, control de acceso físico al sistema, controles de acceso con tarjetas de identificación, control de la temperatura y la humedad de la habitación donde se encuentran los ordenadores.

> **Ejercicios propuestos**
>
> **1.3.1.** Asocia los distintos mecanismos de seguridad expuestos en el tema con los objetivos de la seguridad informática.
>
> **1.3.2.** De las siguientes contraseñas indica cuales se podrían considerar seguras y cuáles no y por qué: a) mesa b) caseta c) c8m4r2nes d) tu primer apellido e) pr0mer1s& f) tu nombre
>
> **1.3.3.** Escribe una contraseña muy segura y di por qué es muy segura
>
> **1.3.4.** Al poner la contraseña de la pregunta anterior, ¿te aseguras al 100% de que nadie va a poder hacer uso de ella (robártela)?

# 1.4 Clasificación de seguridad

Según lo que se protege se puede distinguir entre física y lógica, y dependiendo del momento en el que se actúa entre pasiva y activa.

### 1.4.1 Seguridad física

Es aquella que trata de proteger el hardware de los posibles desastres naturales, incendios, inundaciones, sobrecargar eléctricas, robos... Principales amenazas y mecanismos para salvaguardarnos de ellas:

| Amenaza | Defensa |
|---|---|
| Incendios | Mobiliario ignífugo<br>Evitar localización peligrosa<br>Sistemas antiincendios, detectores de incendios, ... |
| Inundaciones | Evitar plantas bajas<br>Impermeabilización de paredes, techos, sellado de puertas... |
| Robos | Puertas con medidas biométricas, cámaras, vigilantes, ... |
| Señales electromagnéticas | Evitar lugares con radiaciones electromagnéticas<br>Filtros o cableado especial. La fibra óptica no es sensible a esto |
| Apagones | SAI |
| Sobrecargas eléctricas | SAI. También estabilizan la señal eléctrica |
| Desastres naturales | Estar en contacto con los organismos que proporcionan información sobre terremotos o desastres meteorológicos |

### 1.4.2 Seguridad lógica

Complementa a la seguridad física protegiendo el software de los sistemas informáticos.

La seguridad lógica se encarga de controlar que el acceso al software de un sistema informático se realiza por los usuarios adecuados y de la forma correcta.

| Amenaza | Defensa |
|---|---|
| Robos | Cifrado<br>Contraseñas<br>Sistemas biométricos |
| Perdida de información | Copia de seguridad (distintas ubicaciones)<br>Sistemas tolerantes a fallos<br>Discos redundantes |
| Perdida de integridad de la información | Programas de chequeo del equipo<br>Firma digital<br>Comando sfc |
| Entrada de virus | Antivirus |
| Ataques desde la red | Firewall<br>Programas de monitorización<br>Proxys |
| Modificaciones no autorizadas | Contraseñas<br>Listas de control de acceso<br>Cifrar documentos |

> **Ejercicios propuestos**
>
> **1.4.1.** Describe los medios de seguridad física y lógica que hay en el aula.

### 1.4.3 Seguridad activa

Son aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema.

Principales técnicas de seguridad activa:

| Técnicas | ¿Qué previene? |
|---|---|
| Contraseñas | Previene el acceso a recursos a usuarios no autorizados |
| Listas de control de acceso | Previene acceso a ficheros a usuarios no autorizados |
| Encriptación | Evita a personas no autorizadas interpretar la información |
| Software de seguridad | Evita virus y accesos no deseados al sistema |
| Firmas y certificados digitales | Comprueba la procedencia, autenticidad e integridad de los mensajes |
| Sistemas de ficheros tolerantes a fallos | Previene fallos de integridad |
| Cuotas de disco | Previene el uso excesivo de disco por parte de algún usuario |

### 1.4.4 Seguridad pasiva

Comprende el conjunto de medidas utilizadas para que una vez que se produzca el ataque o fallo intentar minimizar los daños y activar los mecanismos de recuperación.

| Técnicas | Resultado |
|---|---|
| Discos redundantes | Restaurar datos que han quedado inconsistentes |
| SAI | Proporcionan energía durante un periodo de tiempo. |
| Copias de seguridad | Podemos recuperar información en caso de pérdida de datos. |

> **Ejercicios propuestos**
>
> **1.4.2.** De cada uno de los elementos expuestos a continuación, indica a qué dos tipos de seguridad están asociados (activa y lógica, activa y física, pasiva y lógica o pasiva y física) a) Ventilador de un equipo informático b) Detector de incendios c) Detector de movimientos d) Cámara de seguridad e) Cortafuegos f) SAI g) Control de acceso mediante el iris del ojo. h) Contraseña para acceder a un equipo i) Control de acceso a un edificio

> **1.4.3.** Evalúa qué medias de seguridad activa y pasiva tienes en torno a tu ordenador personal.

## 1.5. Concepto de vulnerabilidad, malware y exploit.

Como el software está hecho por humanos, puede tener errores. Pueden ser leves (algún mensaje mal traducido), graves (corrupción de datos) o críticos (agujeros de seguridad).

Una **vulnerabilidad** es un defecto en una aplicación que puede ser aprovechado por un atacante que puede programar un **malware** que utilice esa vulnerabilidad para realizar alguna acción no deseada sobre la máquina. (**exploit**)

Hay 3 tipos de vulnerabilidades:

- Vulnerabilidades reconocidas por el suministrador del software y para las cuales ya tiene un parche.
- Vulnerabilidades reconocidas por el suministrador del software y para las cuales no tiene todavía un parche. Algunas veces se proporciona una solución temporal (*workaround*), pero es mejor desactivar el servicio hasta tener el parche que lo solucione.
- Vulnerabilidades no reconocidas por el suministrador del software. Podemos estar expuestos y no ser conscientes de ello.

## 1.6. Tipos de amenazas.

### 1.6.1. Tipos de atacantes

- **Hackers**: Atacan sistemas por curiosidad.
- **Crackers**: Hacker que quiere causar daño u obtener beneficio.
- **Script kiddie**: Aprendices de Hacker y Cracker con pocas habilidades que simplemente se dedican a buscar y lanzar ataques programados por otros sin conocer las consecuencias de los mismos.
- **Sniffers:** Analizan el tráfico de la red para obtener información de los paquetes trasmitidos.
- **Lammers**: Se consideran Hackers pero no tienen suficientes conocimientos para ello.
- **Newbie**: Hacker novato.
- **Ciberterrorista**: Experto informático que trabaja para países u organizaciones como espías o saboteadores.
- **Programadores de virus**: Crean programas dañinos para los sistemas o aplicaciones.
- **Carders**: Atacan sistemas de tarjetas de crédito.

### 1.6.2 Tipos de ataques

- **Spoofing**: Suplanta la identidad de un PC
- **Sniffing**: Analiza el tráfico de red para hacerse con información.
- **Conexión no autorizada**: Se busca un agujero de seguridad y se entra en el sistema.
- **Malware**: Se introducen programas malintencionados en nuestro sistema.
- **Keyloggers**: Almacenan lo que se teclea e incluso hacen capturas de pantalla para averiguar contraseñas.
- **Denegación de servicio (DoS)**: Interrumpe el servicio de servidores o redes.
- **Ingeniería social**: Se obtiene información confidencial de una persona para utilizarla con fines maliciosos.
- **Phishing**: Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o página web.

> **Ejercicios propuestos**
>
> **1.6.1.** Analiza la noticia buscada sobre ataques informáticos e indica el tipo de ataque y atacante del que se trata.

## 1.7 Pautas de protección para nuestro sistema

- Localizar los activos a proteger: equipos, aplicaciones, datos y comunicaciones.
- Redactar y revisar regularmente los planes de actuación ante catástrofes.
- No instalar nada innecesario
- Estar al día de los informes de seguridad que vayan surgiendo y actualizar parches de seguridad
- Formar a los usuarios
- Instalar Firewall
- Llevar una buena política de copias de seguridad
- Gestionar y revisar los logs del sistema.
- Revisar las listas de usuarios activos.

> **Ejercicios propuestos**
>
> **1.7.1.** Analiza que pautas de protección no cumple el sistema que tienes en tu casa.

# 1.8 Ley de protección de datos

La normativa que regula la gestión de los datos personales es la Ley de Protección de Datos de Carácter Personal (LO 15/1999) más conocida como LOPD.

El objetivo de esta ley es garantizar y proteger los derechos fundamentales y la intimidad de las personas físicas. Especifica para qué se pueden usar, cómo deber ser el procedimiento de recogida y los derechos que tienen las personas a las que se refieren entre otros aspectos.

## 1.8.1 Medidas de seguridad

Siempre que se vaya a crear un fichero de datos personales se debe solicitar la aprobación de la Agencia de protección de datos.

En esta solicitud se deben especificar los datos que contendrá el fichero y el nivel de seguridad que se aplicará al fichero.

#### 1.8.1.1 Niveles de seguridad en función de los datos almacenados

- **Básico** : Datos personales
- **Medio**: Referidos a infracciones, gestión tributaria, datos fiscales y financieros. Datos sobre las características y personalidad de los afectados.
- **Alto**: Referidos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

#### 1.8.1.2 Medidas de seguridad para cada nivel

Estas medidas se van acumulando conforme el nivel aumenta.

##### Básico

- Debe existir un documento donde estén reflejadas las funciones y obligaciones de cada usuario del fichero. El responsable del fichero debe almacenar a su vez una lista de los usuarios con sus accesos y las contraseñas deben ser cambiadas en un periodo no superior a un año.
- Debe crearse un registro de incidencias del fichero de datos.
- Cualquier documento que se deseche y que contenga datos de carácter personal tendrá que ser borrado o destruido.
- Las copias de seguridad deberán ser como mínimo una a la semana.

##### Medio

- Al menos una vez cada dos años se realizará un auditoría que verificará los procedimientos de seguridad aplicados.

- Se deben establecer mecanismos para evitar el acceso reiterado no autorizado a los datos y sistemas de control de acceso a los lugares donde se encuentren los equipos con los datos.

**Alto**

- Los datos deben cifrarse para su transporte tanto físico (en un portátil) como por redes públicas o inalámbricas.
- Las copias de seguridad se deben almacenarse en un lugar físico distinto al de los datos.
- Se deben registrar todos los intentos de acceso de los últimos dos años como mínimo.

## 1.9 Normativa de los sistemas de información y comercio electrónico

Regulado por la Comisión del Mercado de las Telecomunicaciones. Ley 34/2002. Aspectos más importantes:

- Las empresas deben proporcionar información sobre nombre, domicilio, dirección de correo electrónico, número de identificación fiscal y precio de los productos.
- Exculpa de responsabilidad siempre que no tengan conocimiento de la información contenida en sus servidores a aquellas empresas que ofrecen alojamiento web.
- Los contratos realizados por vía electrónica son válidos.

> **Ejercicios propuestos**
>
> **1.9.1.** Vamos a crear una empresa de comercio electrónico y vamos a pedir en el registro de los clientes sus datos personales además de sus gustos para enviarles publicidad sobre los temas seleccionados. Indica los pasos a seguir antes, durante y después de la obtención de los datos de los clientes para cumplir la normativa de la LOPD.

## 1.10. Ejercicios de comprobación

**1.10.1.** Asocia las siguientes amenazas con la seguridad lógica y la seguridad física. a) Terremoto b) Subida de tensión c) Virus informático d) Hacker e) Incendio fortuito f) Borrado de información importante

**1.10.2.** Asocia las siguientes medidas de seguridad con la seguridad activa o pasiva. a) Antivirus b) Uso de contraseñas c) Copias de seguridad d) Climatizadores en el CPD e) Uso de redundancia de discos f) Cámaras de seguridad g) Cortafuegos

**1.10.3.** Describe los medios de seguridad activa y pasiva que hay en el aula

**1.10.4.** Ordena de mayor a menor seguridad los siguientes formatos de claves. a) Claves con sólo números b) Claves con números, letras mayúsculas y letras minúsculas c) Claves con números, letras mayúsculas, letras minúsculas y otros caracteres d) Claves con números y letras minúsculas e) Claves con sólo letras minúsculas

**1.10.5.** Busca en Internet las claves más comúnmente usadas.

**1.10.6.** Decides montar una empresa en Internet que se va a dedicar a ofrecer un disco duro on-line. Necesitas de cada usuario: nombre, teléfono y dirección de correo electrónico. ¿En qué afectarán estos datos a la formación de tu empresa? ¿Qué medidas de seguridad tendrás que tomar cuando almacenas esta información?

## 1.11. Bibliografía


- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- García-Cervigón Hurtado, Alfonso et al. Seguridad informática Editorial Paraninfo
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill
- Aplicación de la ley de protección de datos: https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/medidas_seguridad/index-ides-idphp.php
- Oficina de seguridad del internauta: https://www.osi.es/es/contrasenas