CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

ceedcv

CENTRE ESPECÍFIC
D'EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

# UD2. Seguridad y Ética Informática

## 2.1 - Legislación y Protección de la Información.

1) Presta especial atención a los conceptos marcados en amarillo.
2) Amplia información con los APUNTES, foros y en la Red.
3) Practica con los tests de forma periódica durante todo el curso.

**Autores:** Sergio Badal

**Adaptación:** Paco Aldarias

**Fecha**: 23-10-2021

# Índice


1. Ley Orgánica de Protección de Datos
   1.1. Importancia de la protección
   1.2. Novedades de la LOPDGDD
   1.3. Garantía y derechos sobre datos personales
2. Protección de la Información
   2.1. Causas de la pérdida de la información
   2.2. Estrategias de recuperación de la información
   2.3. Herramientas de protección de los equipos informáticos
3. Webgrafía

# 1. LOPD → LOPDGDD

## *Regulación de la Protección de Datos de Carácter Personal.*

***LOPDGDD = Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (2018)***


Protección datos de carácter personal. 1999

Reglamento general de protección de datos europeo. 2018

Ley orgánica española de protección datos de carácter personal y garantías de derechos digitales. 2018

aepd agencia española protección datos

Órgano español de control para que se cumpla la norma.

# 1. LOPDGDD

## 1.1 La importancia de la protección de datos

- Derecho fundamental → art. 10 y 18.4 Constitución Española
- Otorga a las personas físicas el derecho a la intimidad, y establecen que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”
- Facilitamos **datos personales** a empresas privadas y administraciones públicas constantemente (abrir cuenta bancaria, obtener tarjetas descuento, …)
- La constante **evolución de las nuevas tecnologías** → toda la información se encuentre digitalizada → su tráfico resulta mucho más sencillo.

**Normativa necesaria**

Evitar, y/o frenar, el intercambio descontrolado y no autorizado de BBDD digitalizadas con datos de carácter personal.

# 1. LOPDGDD

## 1.2 Novedades de la LOPDGDD

La nueva normativa viene a completar y sustituir a su predecesor, el **Reglamento General de Protección de Datos (RGPD)**.

- El principal objetivo → **incrementar la seguridad jurídica en el ámbito digital**.
- Regula los derechos digitales → adaptación al complejo mundo digital.
- Especial relevancia a los **menores** y a los **trabajadores**.
- Nuevos medios de comunicación → derechos de protección de datos de los usuarios.

# 1. LOPDGDD

**Derecho a la educación digital:** obligación de que el sistema educativo garantice la plena inserción del alumnado en la sociedad digital y el aprendizaje y uso de los medios digitales.

ceedcv
CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

## 1.2 Novedades de la LOPDGDD

**Protección de menores**:

- Se mantiene la especificación de edad y requisitos.
- Delegado de protección de datos. → necesario ppalmente en centros docentes y deportivos.
- Derecho a la educación digital → (*artículo 83)*
- Responsabilidad de los padres o tutores en el uso correcto.

**Relaciones laborales:**

- Informar a los trabajadores de la existencia de sistemas de videovigilancia → de forma **clara, expresa y concisa**.
- No se podrán colocar en lugares de descanso ni en aseos o vestuarios (aunque se encuentren en el interior de la propia empresa)
- Instalación supeditada a cuestiones de seguridad (empresa, productos o empleados)

# 1. LOPDGDD

**SUPRESIÓN**: **Derecho al olvido**.El derecho a solicitar, bajo ciertas condiciones, que los enlaces a tus datos personales no figuren en los resultados de una búsqueda en internet realizada por tu nombre con ciertas limitaciones. Más info: derecho al olvido

En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).

**LIMITACIÓN**: Permitir que se usen pero con ciertas limitaciones

**OPOSICIÓN**: Oponerse al tratamiento de sus datos personales o el cese de éstos AUNQUE no sea necesario su consentimiento

## 1.3 Garantías y derechos sobre nuestros datos personales

### Derechos

LOPD actual (1999 y hasta 05.2018) y Directiva 95/46/CE

| A | R | C | O |
|---|---|---|---|
| Acceso | Rectificación | Cancelación | Oposición |

| Art. 17 | 21 | 20 | 18 | 15 | 16 |
|---|---|---|---|---|---|
| S | O | P | L | A | R |
| Supresión | Oposición | Portabilidad | Limitación | Acceso | Rectificación |

LOPD futura 05.2018 y Reglamento General (UE) 2016/679

Si no se respetan → Solicitud de tutela ante la Agencia Española de Protección de Datos y/o tribunales.

**INDEMNIZACIÓN**.

**EJERCICIO DE DERECHOS**

- Es personal → ejercido directamente por el afectado ante el Responsable.
- No requiere formalismos → remitir por cualquier medio,una solicitud.
- Adjuntar copia del DNI del afectado.

**SEGURIDAD ACTIVA**:
Previene un fallo de seguridad

**SEGURIDAD PASIVA**:
Restaura un fallo de seguridad

ceedcv
CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

# 2. Protección de la Información

**RIESGOS**

- Pérdida de información.
- Fallo en el funcionamiento de componentes.

**NO PUEDEN ELIMINARSE**

**DEBEN REDUCIRSE O MINIMIZARSE**

**3 NIVELES DE SEGURIDAD ACTIVA**

- Protección física
  - Guardias de seguridad.
  - Recintos vigilados.
  - Sistemas antiincendios
- Medidas informáticas
  - Cifrado de información.
  - Cortafuegos.
  - Detectores de intrusos.
  - Antivirus, etc
- Medidas organizativas:
  - Cursos sobre seguridad.
  - Auditorías informáticas.

# 2. Protección de la Información

## 2.1 Posibles causas de pérdida de información.

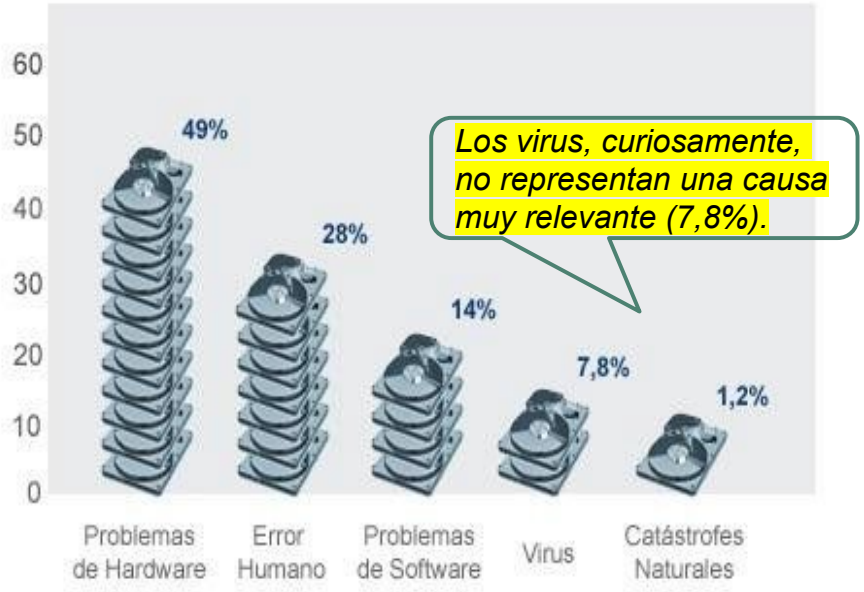
**Pérdida de datos = imposible acceder a datos almacenados informáticamente**

**CAUSAS**

- **Error hardware** → Mal funcionamiento de alguna pieza hardware del sistema de almacenamiento de información.
- **Error humano** → Pérdida de información debida a un error humano ya sea fortuíto o intencionado (formateos, borrados, etc.)
- **Error software** → Pérdida de datos causados por los propios programas informáticos (mala instalación, funcionamiento incorrecto, etc.)
- **Virus**. El ataque de virus informáticos puede producirse de múltiples formas y afectar de manera distinta a la información almacenada.
- **Catástrofes naturales**. Las catástrofes naturales pueden causar graves pérdidas de información en equipos informáticos (inundaciones, fuegos, etc.)

# 2. Protección de la Información

## 2.1 Posibles causas de pérdida de información.




Casi la mitad de las pérdidas son debidas a a fallos de HW (HDs, memoria, placa...)!

- Picos de tensión → avería en la fuente de alimentación o una sobrecarga de la red, que quema la electrónica de un dispositivo.
- Averías mecánicas (piezas móviles) → dilataciones y contracciones por calentamiento durante su uso.

**IMPORTANTE CONCLUSIÓN:**
**ES CASI MÁS IMPORTANTE PROTEGER Y CUIDAR EL HW QUE EL SW!**

# 2. Protección de la Información

## 2.2 Estrategias de RECUPERACIÓN de la información **(S.PASIVA)**

**(1)** Los virus informáticos son el tipo más común de malware, por lo que es habitual ese nombre para denominar a todos los tipos de programas hostiles, a todo el malware, o **a todo el que no tiene un nombre específico**.

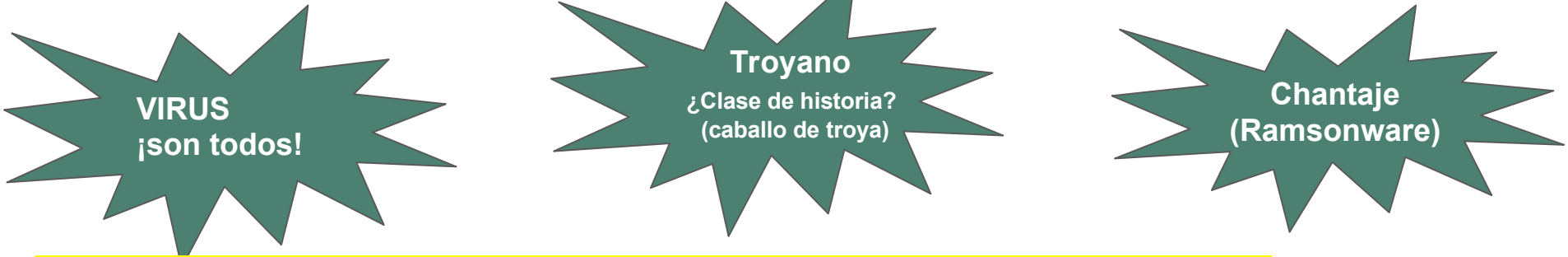
ceedcv
CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

# 2. Protección de la Información

## 2.3 Herramientas de protección de equipos informáticos (S.ACTIVA)

**Malware** = programa cuya finalidad es infiltrarse/dañar un ordenador sin el conocimiento del propietario

- **VIRUS (1)**
- **ADWARE** publicidad
- **TROYANO** Lo vemos en la parte 2 del tema
- **GUSANO (2)** Se reproduce infinitamente
- **SPYWARE** Lo vemos luego...
- **RAMSONWARE**




**(2)** Los **gusanos/worms** son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

**Todos los antivirus suelen ser 3 en 1** y tener funciones básicas de antivirus (genérico), antispyware y de antispam pero es recomendable instalar un antivirus (genérico) y un antispyware y un antispam especializados.

ceedcv
CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

# 2. Protección de la Información

## 2.3 Herramientas de protección de equipos informáticos **(S.ACTIVA)**

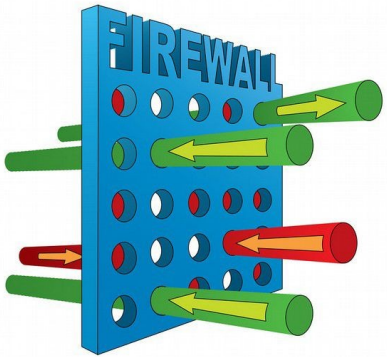
**ANTIVIRUS**

**ANTISPYWARE**

**ANTISPAM**
Lo vemos en la parte 2 del tema

**CORTAFUEGOS**





# 2. Protección de la Información

## 2.3 Herramientas de protección de equipos informáticos **(S.ACTIVA)**

**ANTIVIRUS**

- OBJETIVO → Analizar todo el tráfico que entra y sale de la red y comprobar si tiene virus (correo electrónico y la navegación por Internet) **ANALIZA QUÉ ENTRA/SALE**.
- En permanente actualización → conectados a la BBDD para antídoto de nuevos virus. **Si sale un nuevo virus y no actualizo mi antivirus me podré infectar.**
- Mecanismos básicos de detección de amenazas:
  - **Comparación** → búsqueda de patrones de código coincidentes con la BBDD de virus conocidos.
  - **Detección programas hostiles por comportamiento**
- Cuando se detecta (TÚ DECIDES):
  - Eliminar el software dañino (lo más común)
  - Poner en cuarentena
  - No hacer nada (confiar).

# 2. Protección de la Información

## 2.3 Herramientas de protección de equipos informáticos **(S.ACTIVA)**

**ANTISPYWARE**

**SPYWARE = malware** que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

- **Se autoinstala** de forma que se ejecuta cada vez que se pone en marcha el ordenador.
- Funciona todo el tiempo, controlando el uso que se hace de Internet.
- No se intenta replicar en otros ordenadores → funciona como un parásito.
- Consecuencias (aparte de las cuestiones de privacidad):
  - Pérdida del rendimiento del sistema (¡TU PC TRABAJA PARA SU CREADOR!)
  - Problemas de estabilidad graves (el ordenador se queda "colgado").
  - Dificultad a la hora de conectar a Internet.

- ANALIZA QUIEN ENTRA Y SALE DE TU PC Y DESDE DÓNDE VIENE O A DÓNDE VA

ceedcv
CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

# 2. Protección de la Información

## 2.3 Herramientas de protección de equipos informáticos (S.ACTIVA)

**CORTAFUEGOS**

- Encargado de controlar y filtrar las conexiones de red
- Mecanismo básico de prevención contra amenazas de intrusión externa.
- Barrera de protección entre un equipo o red privada y el mundo exterior.
- Controla el acceso de E/S al exterior, filtra las comunicaciones, registra los eventos y genera alarmas.
- Un cortafuegos permite:
  - Bloquear el acceso a determinadas páginas de Internet (por ejemplo, algunas de uso interno de una empresa).
  - Monitorizar las comunicaciones entre la red interna y externa.
  - Controlar el acceso a determinado servicios externos desde dentro de una empresa.
- Separar distintas subredes dentro de una gran empresa.

  *Por ejemplo, se podrían aislar los ordenadores que gestionan las nóminas del resto de la red de la empresa (para evitar que un empleado de la empresa pueda entrar en el ordenador de nóminas y se modifique su nómina, o pueda consultar la nómina del director general).*

# 7. Webgrafía


1. https://www.aepd.es/
2. • https://a-lign.com/types-malware-prevent-malware-attacks
3. • https://es.wikipedia.org/wiki/Bot
4. • https://www.gextor.es/la-nueva-lopd-rgpd-en-espana/
5. • https://protecciondatos-lopd.com/empresas/derechos-arco-que-son/

## 2.4 Actividades

- ☐ Busca y compara las características (Precio y capacidad) de 3 servicios para realizar Copias de Seguridad en la nube:
  - ▷ RESPUESTA: Artículos web de ejemplo: Xataka , PcWorld

- ☐ Comprueba qué tipo de antivirus tienes instalado en tu ordenador y que cumpla las siguientes características:
  - ▷ Capacidad de detención de virus
  - ▷ Capacidad de eliminación de infecciones
  - ▷ Capacidad actualización de las bases de datos para detectar nuevos virus
  - ▷ Integración con el correo electrónico
  - ▷ Capacidad de detención de otros tipos de malware y peligros como Spam, spyware, phishing…
  - ▷ Servicio de atención al cliente y apoyo técnico: