CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

UD 2.1

LEGISLACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCIA DIGITAL (TICD)
21/22
FORMACIÓN DE PERSONAS ADULTAS / ACCESO A CFGS

Autor: Paco Aldarias
paco.aldarias@ceedcv.es
Fecha: 23-10-2021

Adaptación de los apuntes de Sergio Badal

Licencia

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

ÍNDICE DE CONTENIDO

UD02.1. LEGISLACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

1. LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES

Todas las cuestiones relativas a la Protección de Datos de Carácter Personal se encuentran reguladas por la LOPDGDD (*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales*).

Esta Ley entró en vigor el pasado 6 de Diciembre, quedando derogada la anterior LOPD (*Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*).

Se trata de una adaptación de la legislación española al RGPD (*Reglamento (UE) 2016/679, General de Protección de Datos Personales*) del Parlamento Europeo.

Este reglamento, que entró en vigor el 25 de mayo de 2018, es relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que se aplica directamente a todos los Estados miembros de la Unión Europea derogando sus legislaciones en todo lo que sea contrario a su regulación. No es que queden totalmente derogadas estas normas, sino que subsisten en cuanto no contradigan al Reglamento Europeo.

Introduce una sola normativa para toda los Estados de la Unión Europea, buscando la adaptación continúa a los cambios tecnológicos y la unificación de la materia en todos los países.

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, con carácter general es la Agencia Española de Protección de Datos (AEPD), existiendo otras Agencias de Protección de Datos de carácter autonómico, en las Comunidades Autónomas de Cataluña y en el País Vasco.

1.1 Importancia de la protección de datos

La protección de los datos de carácter personal es un **derecho fundamental** que encuentra su origen normativo en los artículos 10 y 18.4 de la **Constitución Española**, que otorgan 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."

Cualquier persona constantemente facilita datos de carácter personal a empresas privadas y administraciones públicas, ya sea para abrir una cuenta bancaria, para obtener una tarjeta de descuento o para solicitar una licencia de obras a nuestro Ayuntamiento.

La constante evolución de las nuevas tecnologías conlleva inevitablemente que toda la información se encuentre digitalizada, por lo que su tráfico, incluso a nivel global resulta mucho más sencillo. Los gobiernos nacionales y, en especial la Unión Europea, han iniciado acciones conjuntas de cara a evitar, o en su caso frenar, el intercambio descontrolado y no autorizado de base de datos digitalizadas que contengan datos de carácter personal.

1.2 Principales novedades de la LOPDGDD

La nueva normativa se basa, amplia y adapta en el **Reglamento General de Protección de Datos (RGPD)**.

El principal objetivo es **incrementar la seguridad jurídica en el ámbito digital**. Pero no es lo único que se pretende conseguir.

Por primera vez, se regulan en nuestro país los derechos digitales. Y se hace con la intención reinterpretar nuestro sistema de derechos fundamentales para que se adapte al complejo mundo digital.

Se busca dar una especial relevancia a los **menores** y a los **trabajadores**. También se trata el impacto de los nuevos medios de comunicación, y cómo los usuarios pueden ejercer sus derechos de protección de datos en este contexto.

Las **novedades** que introduce la nueva **LOPDRGG** respecto al **RGPD,** y que deben ser conocidas tanto por usuarios como por responsables de la protección de datos personales en empresas e instituciones, son las siguientes:

- Se amplían los **principios aplicables** a la protección de datos:
  - Necesidad de que los datos personales sean siempre **exactos y veraces**.
  - Se amplía **el principio de confidencialidad,** vigente incluso cuando la relación entre el responsable del tratamiento de los datos y el usuario haya finalizado.
  - El **consentimiento** deberá ser, explícito y adecuado. Es decir, que los datos personales no podrán ser utilizados para otros fines que no sean los especificados.
- La responsabilidad de los encargados del tratamiento de los datos. Se ha visto ampliado a aquellas situaciones en las que se pueda producir algún tipo de **daño moral, social o económico** significativo (Ej: fraude, discriminación, usurpación de la identidad o pérdida financiera).
- Las **infracciones** por incumplimiento:
  - Se distingue entre **infracciones leves, graves y muy graves**.
  - La cuantía continúan siendo las especificadas en el RGPD, pero cambian los **plazos de prescripción: Artículo 78 de la LOPDGDD**: "*las sanciones por importe igual o inferior a 40.000 euros prescriben en el plazo de un año, las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años y las sanciones por un importe superior a 300.000 euros prescriben a los tres años*".

- La protección de datos en el caso de los **menores**:
  - Se mantiene la especificación relativa a la edad y a los requisitos
  - Se establece un **delegado de protección de datos**. Esto es especialmente necesario, y así lo recoge la nueva ley, en el caso de **centros docentes y deportivos**.
  - El **derecho a la educación digital**, contemplado en el **artículo 83**: "*El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso*".
  - Se señala la **responsabilidad de los padres o tutores** en el uso correcto y equilibrado de esos medios digitales.
- El impacto de la nueva normativa en las **relaciones laborales**:
  - Necesidad de informar a los trabajadores acerca de la existencia de sistemas videovigilancia, de forma **clara, expresa y concisa**.
  - No se podrán colocar grabadores de vídeo o audio en lugares de descanso ni en aseos o vestuarios (aunque se encuentren en el interior de la propia empresa)
  - Su instalación estará supeditada a cuestiones de seguridad (de la propia empresa, la de sus productos o la de los empleados).

1.3 Garantías y derechos sobre nuestros datos de carácter personal

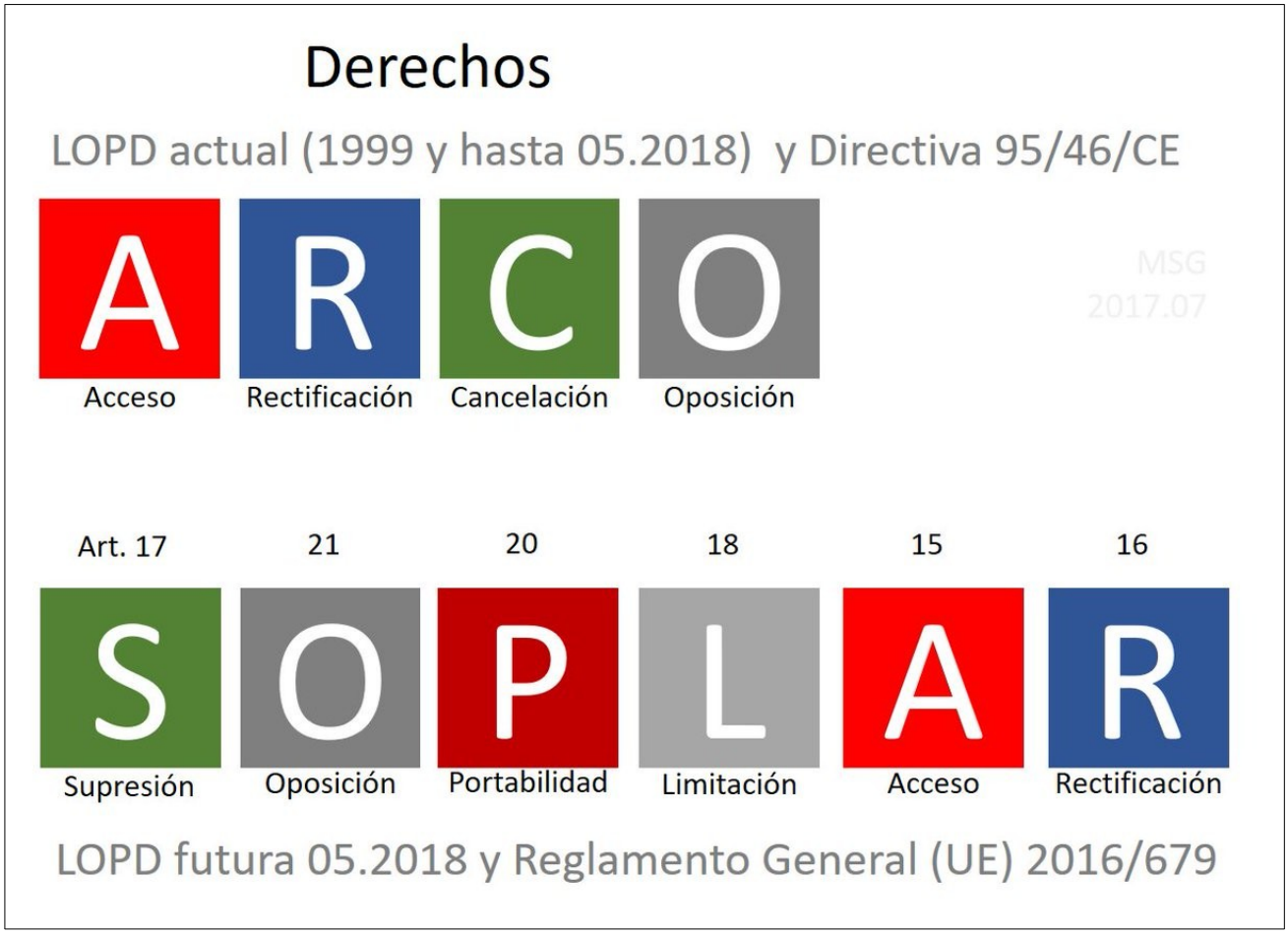
Toda persona física dispone de una serie de derechos respecto a sus datos de carácter personal.

Son cuatro los derechos que preveía la normativa, los llamados derechos **ARCO**:

- **Derecho de Acceso**: Se le reconoce, en primer lugar, un derecho de acceso a sus datos que se relaciona con su derecho a la información sobre el tratamiento que se está haciendo de dichos datos.
- **Derecho de Rectificación**: Se le reconoce el derecho a la rectificación, oposición, portabilidad y supresión de sus datos personales.
- **Derecho de Cancelación**: En relación con el derecho de supresión, una vez dado nuestro consentimiento para una finalidad concreta, por ejemplo, que envíen información sobre un tipo de productos, tiene el derecho de suprimir dicho consentimiento con la misma facilidad que lo dio.
- **Derecho de Oposición**: Se trata del derecho de una persona a oponerse al tratamiento de sus datos personales o el cese de éstos en los casos:
  - que no sea necesario su consentimiento,
  - en los que los ficheros se usen con finalidades publicitarias,
  - o que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado.

Como anteriormente se comentó, la nueva normativa amplia estos derechos.

- **Derecho a la portabilidad de los datos:** El derecho a la portabilidad de datos es una de las novedades que trae el reglamento. En resumen es, la traslación de la portabilidad en telefonía móvil, al mundo de la privacidad.
- **Derecho al olvido:** Este derecho es una de las mayores novedades de este reglamento. Se trata de la supresión de los datos personales del interesado sin dilación siempre y cuando dichos datos cumplan ciertas condiciones.



Por último, si no se han respetado los derechos en la materia, se les reconoce la opción de **solicitar la tutela** efectiva ante la Agencia Española de Protección de Datos y/o antes los tribunales, donde se puede obtener, si se confirma la vulneración, una indemnización.

El ejercicio de cualquiera de estos derechos es personal, y debe ser ejercido directamente por el afectado (titular de los datos de carácter personal) ante el Responsable del Fichero.

El ejercicio de los derechos no requiere de ningún formalismo concreto, sino que basta con remitir, por cualquier medio, la solicitud de ejercicio del mismo.

El único requisito adicional que puede exigirse es que la solicitud vaya acompañada de una copia del DNI del titular de los datos, de forma que el responsable del fichero pueda corroborar la identidad del solicitante, cumpliendo así con el principio de calidad.

Si el responsable del fichero no cumpliera con los plazos, el afectado puede denunciar a la Agencia Española de Protección de Datos, incluyendo toda la documentación relativa a la solicitud realizada al responsable del fichero.

2. PROTECCIÓN DE LA INFORMACIÓN

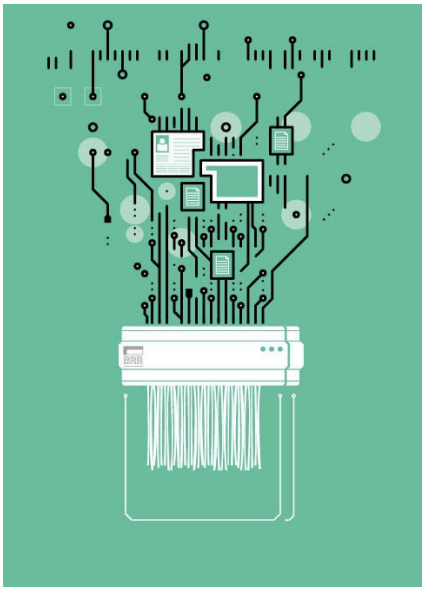


Figura 1: "Security data" by Alain Bousquet - licensed CC BY-NC-SA 4.0

Los equipos informáticos están expuestos a multitud de **riesgos**, algunos internos, como la pérdida de información o el incorrecto funcionamiento de alguna de sus partes, y otros que provienen del exterior, consecuencia de su conexión a redes, especialmente a Internet.

El nivel de riesgo, además, es diferente si hablamos de ordenadores que forman parte de una organización, de una empresa o consideramos equipos informáticos de uso personal.

Los riesgos a los que se enfrenta un equipo informático **no pueden ser totalmente eliminados**, sino que pueden ser reducidos. Por ello, la seguridad en un sistema informático tiene que basarse en objetivos realistas .

Existen tres **niveles** a los que puede actuarse con objeto de **minimizar** los riesgos:

- **Protección física**: Guardias de seguridad, recintos vigilados, sistemas antiincendios (de nada vale poner medidas de seguridad informática si cualquier persona puede entrar en un recinto y robar un ordenador vital de una empresa, por ejemplo).
- **Medidas informáticas**: son los sistemas y soluciones informáticas que aumentan la seguridad de los sistemas informáticos. Estos incluyen el cifrado de la información, cortafuegos, antivirus, detectores de intrusos, etc.
- **Medidas organizativas**: Si consideramos los equipos informáticos de una organización o empresa, son necesarios cursos de formación sobre seguridad, auditorías informáticas, etc. para que todos los usuarios de los equipos sean conscientes de los riesgos y sepan actuar correctamente.

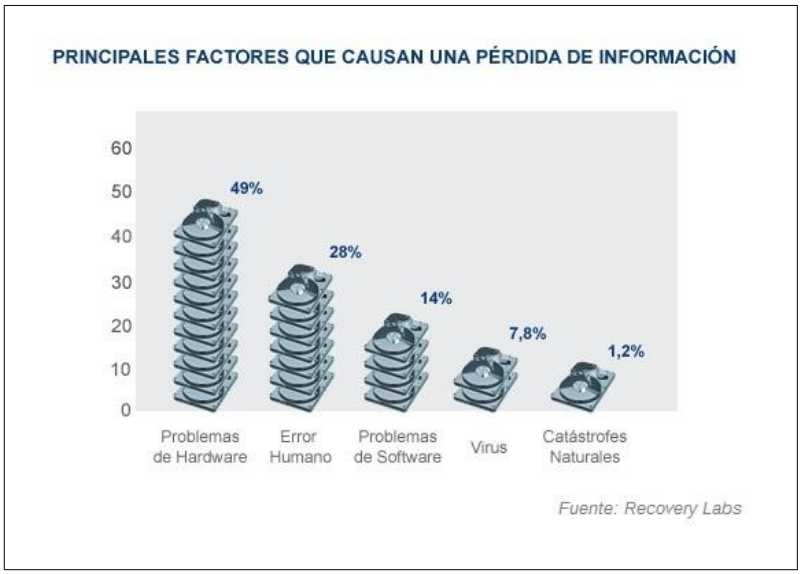
2.1 Posibles causas de la pérdida de información

Una pérdida de datos, es aquella situación en la que no podemos acceder a datos importantes almacenados en un sistema informático.

Se puede producir por varias **causas**:

- **Error del hardware**. Este tipo de fallos se producen por el mal funcionamiento de cualquier pieza del hardware del que se compone un sistema de almacenamiento de información
- **Error humano**. Toda pérdida de información que sea debida a un error humano ya sea intencionado o fortuíto (formateos, borrados, etc.)
- **Error del software**. En ocasiones son los propios programas informáticos los que causan la pérdida de datos, ya sea por una mala instalación, por 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.)

Casi la mitad de las pérdidas de datos que se producen son debidas a **errores de funcionamiento de los discos duros**, siendo el **error humano** la segunda causa en importancia. Los virus, curiosamente, no representan una causa muy relevante (7,8%).



Las causas que pueden dañar un disco duro son variadas. Una de ellas son los picos de tensión, que se producen cuando una avería en la fuente de alimentación o una sobrecarga de la red eléctrica ocasionan una subida de tensión que quema la electrónica de un dispositivo.

Otro tipo de averías del disco duro son las averías mecánicas. Los discos duros tienen piezas móviles, que se pueden dañar como cualquier otro aparato. Los problemas mecánicos más comunes vienen provocados por las continuas dilataciones y contracciones del disco duro, debidas al proceso sucesivo de calentamiento y enfriamiento de los dispositivos.

La más famosa de la averías que afectan a los cabezales es conocida como aterrizaje, o técnicamente "head crash". Esta avería consiste, en que las cabezas acumulan un exceso de partículas en la zona que está en contacto con el soporte magnético, y acaban erosionándola, con lo que todo el esmalte magnético que contenía los datos desaparece, quedando solo el aluminio de los platos. Responsables frecuentes de estos casos suelen ser el desgaste de los discos, la acumulación de humedad o humo de tabaco.

2.2 Estrategias de prevención de pérdida de información

2.2.1 Copias de seguridad (Backup)

Las copias de seguridad son una medida para recuperarse de un desastre (perdida voluntaria o involuntaria de información, ordenador estropeado, catástrofe natural, etc.), Por ello, es de vital importancia que las copias de seguridad estén perfectamente **planificadas** y que se **verifique** el correcto funcionamiento de la copia.

Figura 2: "Backups-9554" by DonJinTX - CC BY-NC 2.0

Reciben el nombre también de copias de respaldo o backup.

También es importante que los soportes físicos de estas copias de seguridad se custodien de forma adecuada.

La copia de seguridad suele ser **únicamente** de los **datos** , no de los programas, y suele incluir carpetas y archivos del usuario, favoritos , correo electrónico, etc. Hay también la opción de hacer una copia exacta, llamada **imagen**, de toda la información de un disco duro en un sólo bloque.

Existe una gran gama de **software** en el mercado para realizar copias de seguridad. Es importante definir previamente los requerimientos específicos para determinar el software adecuado. Existe una infinidad de programas adaptados a cada necesidad.

En la actualidad, a los medios tradicionales como los discos duros y los formatos ópticos o de cinta se han incorporado los diferentes servicios de **almacenamiento en la nube** que nos permiten de forma gratuita o por un pequeño coste guardar decenas de gigas en servidores remotos que se supone tienen un grado de seguridad mayor que el que podríamos tener en casa.

Ventajas de guardar archivos en la nube:

- Las copias se hacen automáticamente del ordenador a un servicio remoto de backup online.
- Puedes acceder en cuestión de minutos y recuperar los datos desde otro ordenador.

Desventajas de guardar los archivos online:

- La nube implica poner tus archivos en manos de un servidor externo.
- No todos los servios de backup te facilitan cumplir con la LOPDGDD para alojar archivos de terceros con seguridad.

Por eso, si nos decidimos por esta opción, es importante elegir bien el servicio que vamos a utilizar y asegurarnos de que cumple con nuestras expectativas y necesidades concretas. Una alternativa, o más bien, complemento, es un soporte físico local.

2.2.2 Restauración

El proceso de copia de seguridad se complementa con otro conocido como restauración de los datos (en inglés restore), que es la acción de **recuperar** los datos de la copia de seguridad.

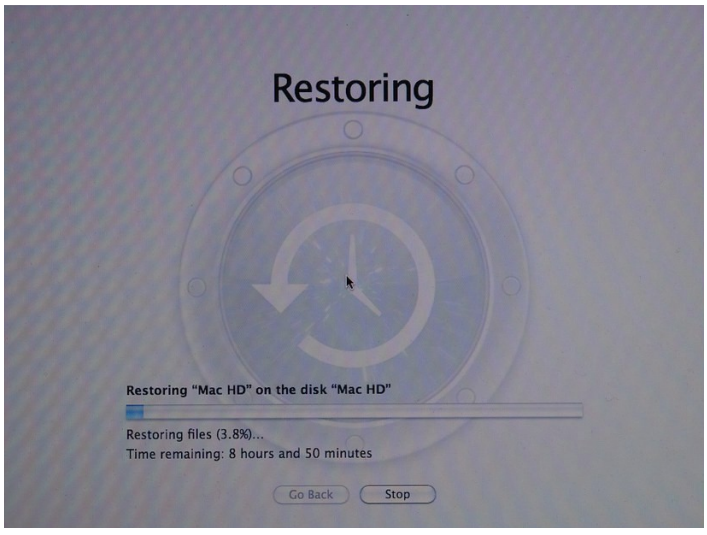


Figura 3: "DSC04880" by RJL20 - CC BY-SA 2.0

En el caso de que se produzca un bloqueo del sistema operativo, también existe la posibilidad de restaurarlo. Para ello, la mayoría de los fabricantes de ordenadores incluyen un disco de restauración del sistema con cada equipo. Estos discos son relativamente rápidos y eficaces en restaurar el sistema a su **estado inicial**. No obstante, este "estado limpio" inicial, se hace de modo que se borran los datos de usuario, los parámetros de los programas, los marcadores, los documentos y otros archivos importantes.

Si disponemos de una copia de seguridad de los datos es posible retornar a nuestro ordenador al punto anterior al fallo.

2.3 Herramientas de protección de los equipos informáticos

Se denomina "**malware**" al programa cuya finalidad es infiltrarse o dañar un ordenador sin el conocimiento del dueño. Son programas «disfrazados» con el objetivo de engañar al usuario.

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, aunque hay muchos mas tipos: Virus, Adware, Trojan, Worms, Spyware, Ramsonware.

Cuando surgieron los virus estos eran una **demostración** de la **habilidad** de sus programadores. Posteriormente, el malware producía efectos muy visibles en los equipos (apagar el ordenador, cambiar caracteres, borrar archivos...).

Hoy en día el hay varios tipos malware y sus uso se han diversificado para:

- **Robar información** (Spyware) como datos personales, contraseñas, nº de cuentas bancarias.
- Crear redes de **ordenadores zombies o botnet** (Virus, Adware, Trojan, Worms) para utilizarlos para el envío masivo de spam, phishing o realización de ataques de denegación de servicio.
- Realizar **chantaje** (Ramsonware) y vender falsas soluciones de seguridad para solucionar el problema. Por ejemplo, nos dicen que tenemos un virus y que hay que pagar una cantidad para conseguir el programa para eliminarlo o no dejar arrancar el equipo o cifrar el contenido de determinados archivos y solicitar un pago para solucionarlo.

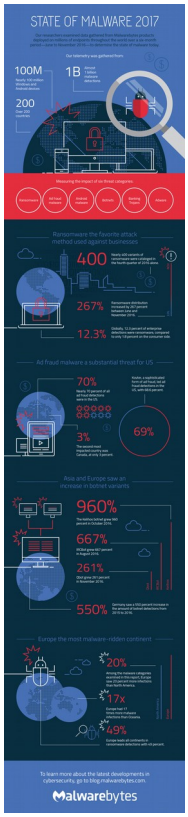


Figura 4:
"State of Malware 2017" by Infographic
Box CC BY-NC-ND 4.0

2.3.1 Antivirus

El objetivo de un antivirus es la de **analizar** todo el tráfico que entra y sale de la red y **comprobar** si tiene virus. Lo más habitual es analizar únicamente el tipo de tráfico que puede introducir virus: el correo electrónico y la navegación por Internet.

Estos antivirus están en **permanente actualización**: están conectados a la bases de datos de la empresa fabricante con lo que si aparece un nuevo virus y se descubre su antídoto, rápidamente el antivirus lo podrá interceptar evitando así su propagación.

Tienen dos mecanismos básicos de detección de amenazas:

- **Comparación**, buscando entre los programas el patrón de código que coincida con los almacenados en una biblioteca de patrones de virus conocidos.
- Detección de programas hostiles basados en el **comportamiento**. El antivirus conoce una serie de comportamientos sospechosos y estudia a los programas que, por su código, estén preparados para llevarlos a cabo.

Cuando se detecta alguno, lo más común es eliminar el software dañino, aunque también se puede poner en cuarentena o no hacer nada, pues hay veces que se pueden producir confusiones.

2.3.2 Antiespías (AntiSpyware)

Aunque hoy en día los antivirus tratan de ampliar su protección hacia cualquier tipo de malware, en ocasiones es necesario utilizar **programas específicos** para detectar el spyware, que complementan la actividad del antivirus.

El **spyware** o programa espía es un 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.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM), y funciona todo el tiempo, controlando el uso que se hace de Internet. Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un **parásito**.

Las **consecuencias** de una infección de spyware moderada o severa (aparte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del **rendimiento** del sistema (hasta un 50 % en casos extremos), y problemas de **estabilidad** graves (el ordenador se queda "colgado"). También causan dificultad a la hora de conectar a Internet.

2.3.3 Cortafuegos (Firewalls)

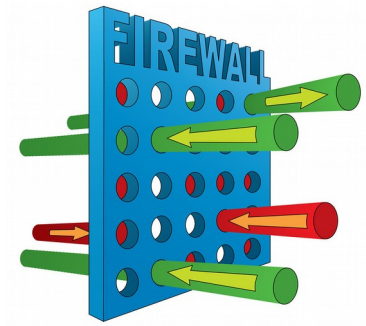


Figura 5: "What-on-Earth-is-a-firewall" by Adlopa CC BY-NC-ND 2.0

Un cortafuegos o firewall es un elemento encargado de **controlar y filtrar las conexiones de red** de una máquina o conjunto de máquinas.

Se trata de un mecanismo básico de **prevención** contra amenazas de intrusión externa. Supone la barrera de protección entre un equipo o red privada y el mundo exterior. Controla el acceso de entrada y salida 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 (por ejemplo, puede evitar que los empleados de una empresa usen Internet para descargarse ficheros).

Los cortafuegos también se pueden usar para **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).

Con posterioridad a los cortafuegos en red se desarrollaron los cortafuegos , por el gran incremento del número de ordenadores domésticos conectados permanentemente a Internet (vía ADSL, cabla-módem, etc.)

2.3.4 Antispam

Figura 6: "SPAM" by AJC1 is licensed under CC BY-NC 2.0

El antispam es lo que se conoce como método para **prevenir** el correo basura o spam (origen del término). También hay más tipos de spam aparte del correo, como el que se genera en los grupos de las plataformas de mensajería instantánea, donde se introducen programas automatizados llamados bots para generar mensajes de publicidad no deseada.

Tanto los usuarios finales como los administradores de sistemas de correo electrónico utilizan **diversas técnicas** contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software (los AntiSpam) para aliviar la carga que cae sobre usuarios y administradores.

Técnicas locales: Las que se realizan en el propio ordenador del usuario.

- Emplear un **diccionario** propio para detectar palabras que suelen aparecer en estos correos. Ese diccionario puede ser "creado" con palabras que el propio usuario identifica como spam manualmente, o de forma inteligente por la aplicación, cuando el usuario selecciona qué es deseado y qué es no deseado de su bandeja de entrada.
- Otra es el uso de una **lista** de amigos y una lista de enemigos. El programa o el propio usuario manualmente identifica las direcciones y nombres que son considerados amigos y de los cuales no recibirán correos no deseados. Lo mismo para la lista de enemigos.

Técnicas no locales: La utilizan las herramientas que se conectan a servidores remotos, que se encargan de analizar cada uno de los emails que llegan al usuario, para identificar si son o no spam.

- Esos servidores remotos utilizan grandes **bases de datos** con información (direcciones IP, nombres, textos, etc.) para identificar el correo no deseado.

No existe la fórmula perfecta para solucionar el problema del spam por lo que entre las múltiples existentes unas funcionan mejor que otras, rechazando así, en algunos casos, el correo deseado para eliminar completamente el spam, con los costes que conlleva de tiempo y esfuerzo.

El principal objetivo de una herramienta antispam es lograr un **buen porcentaje de filtrado** de correo no deseado. Pero tampoco deben **identificar al correo deseado como no deseado**, pues eso traería peores consecuencias que "olvidar" filtrar algún spam.

Algunos antivirus y firewalls (cortafuegos) poseen incorporadas herramientas antispam.

Aunque no lo parezca, el impacto que tiene el Spam es mucho mayor de lo que podemos suponer a primera vista. Hasta el 85% del tráfico ha llegado a ser spam: https://www.europapress.es/portaltic/ciberseguridad/noticia-spam-supuesto-85-todo-correo-electronico-mundo-mes-abril-20190617170925.html

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:

3. BIBLIOGRAFÍA

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