

Desarrollo de Competencias Digitales

Seguridad informática



Miquel Mazuque Periz

ÍNDICE:

1.	Conceptos de seguridad	1
1.1.	Amenazas para los datos	1
1.1.1.	Datos e información	1
1.1.2.	Delito informático	2
1.1.3.	Hackear, crackear y hacking ético	2
1.1.4.	Tipos de amenazas para los datos	2
1.2.	Valor de la información.....	3
1.2.1.	Motivos para proteger la información personal y la comercialmente delicada	3
1.2.2.	Medidas para evitar el acceso no autorizado a datos	4
1.2.3.	Características básicas de seguridad de la información	5
1.2.4.	Requisitos de protección, almacenamiento y control de datos/privacidad en el país	5
1.3.	Seguridad personal	6
1.3.1.	Ingeniería social: phishing, shoulder surfing,	6
1.3.2.	Robo de identidad.....	6
1.4.	Seguridad de un archivo	7
1.4.1.	Macros.....	7
1.4.2.	Establecer una contraseña.....	8
1.4.3.	Cifrado	9
1.4.4.	Compresión de archivos.....	11
1.4.5.	Proteger un archivo con su aplicación	11
1.4.6.	Keyloggers	11
2.	Malware	12
2.1.	Definición, función y tipos	12
2.2.	Protección	13
2.2.1.	Cómo funciona un virus	13
2.2.2.	Síntomas que indican la presencia de virus informáticos.....	14
2.2.3.	Cómo funciona un software de antivirus y sus limitaciones.....	15
2.2.4.	Antivirus de pago y gratuitos	15
2.2.5.	Analizar unidades, carpetas y archivos específicos	16
2.2.6.	Cuarentena.....	16
3.	Seguridad de la red	17
3.1.	Redes	17
3.1.1.	Conceptos	17
3.1.2.	Rol del administrador de la red.....	18
3.1.3.	Firewall (servidor de seguridad).....	18
3.2.	Conexiones de red	19
3.2.1.	Tipos de conexión	19
3.2.2.	Implicaciones para la seguridad.....	21
3.3.	Seguridad inalámbrica	22
3.3.1.	Conectarse a una red inalámbrica	22
3.3.2.	Proteger el acceso a una red inalámbrica	23

3.3.3.	Tipos de seguridad inalámbrica	24
3.3.4.	Riesgos de una red inalámbrica sin protección	26
3.3.5.	Técnicas de seguridad biométrica.....	27
4.	Uso seguro de la Web.....	28
4.1.	Conveniencia de hacer actividades en línea en sitios Web seguros	28
4.2.	Pharming.....	29
4.3.	Certificado digital	30
4.4.	Contraseña de un solo uso	30
4.5.	Autocompletado en un formulario	31
4.6.	Cookies	33
4.7.	Software para controlar contenidos de Internet	37
4.7.1.	Configurar el Control parental	37
4.7.2.	Administrar las cuentas añadidas al Control parental	38
4.7.3.	Gestionar la cuenta de un menor	39
4.7.4.	El control parental en Windows 7.....	41
4.8.	Redes sociales	43
5.	Comunicaciones.....	45
5.1.	Correo electrónico	45
5.1.1.	Cifrado/descifrado de un correo electrónico.....	45
5.1.2.	Firma digital	46
5.1.3.	Correos electrónicos fraudulentos y no solicitados.....	46
5.1.4.	Phishing	46
5.1.5.	Peligro al abrir un archivo adjunto.....	47
5.2.	Mensajería instantánea	47
5.2.1.	Concepto y uso.....	47
5.2.2.	Vulnerabilidades de seguridad de la MI.....	48
6.	Gestión de datos seguros	49
6.1.	Copia de seguridad de los datos	49
6.1.1.	Seguridad física de los dispositivos	49
6.1.2.	Herramientas de copia de seguridad en Windows	50
6.1.3.	Hacer una copia de seguridad periódica.....	51
6.1.4.	Restaurar los datos respaldados	55
6.1.5.	Crear una imagen del sistema.....	56
6.1.6.	Restaurar el equipo a partir de una imagen del sistema	57
6.2.	Destrucción segura	58
6.2.1.	¿Qué datos hay que eliminar de dispositivos de manera permanente?	58
6.2.2.	Diferencia entre eliminar y destruir datos de manera permanente.....	59
6.2.3.	Métodos para destruir de manera permanente datos digitales.....	59

1. CONCEPTOS DE SEGURIDAD

Seguridad e Informática son dos conceptos que nos cuesta mucho poner juntos. Nadie puede garantizarnos una seguridad total cuando usamos las Tecnologías de la Información y la Comunicación (TIC) pero, igual que en cualquier otro aspecto de nuestra vida, si nos informamos de los peligros a los que nos exponemos y tomamos unas precauciones básicas, podemos reducir al mínimo los riesgos del uso de las TIC.

Este es el objetivo de este curso, mostrar los riesgos a los que nos enfrentamos y cómo poder evitarlos. Este curso está dirigido a un usuario de las TIC, no a un “informático” y, por lo tanto, intentaremos dar las explicaciones de la manera más sencilla posible.

El tema puede ser aburrido pero vale la pena si queremos tener un mínimo de seguridad a la hora de usar las TIC.

En este primer capítulo veremos los conceptos clave relacionados con la seguridad.

1.1. AMENAZAS PARA LOS DATOS

Nuestros datos (personales o de empresa) están expuestos a muchas amenazas: fallos de software, averías de los discos duros, errores humanos, virus, accesos de personas con malas intenciones, fallos eléctricos, robos, incendios, inundaciones, ...

Si no tomamos las precauciones adecuadas, cualquiera de estas amenazas puede hacer que perdamos información o que alguien (no deseado) acceda a ella.

1.1.1. Datos e información

Los **datos** son símbolos que describen algo. Un dato puede ser una letra, un número, un signo ortográfico o cualquier otro símbolo. Los datos no contienen ninguna información, por sí solos no tienen sentido. Los datos se convierten en información cuando se asocian dentro de un contexto. Para ser útiles, los datos deben convertirse en información y ofrecer así un significado, conocimiento, ideas o conclusiones. Por sí mismos, los datos no tienen capacidad de comunicar un significado.

La **información** es un conjunto organizado de datos que transmite un significado.

Diferencias entre dato e información:

Dato	Información
Representación simbólica	Conjunto de datos procesados
No tiene sentido semántico	Tiene un significado
No transmite mensaje	Transmite un mensaje
No incrementa el conocimiento	Incrementa el conocimiento

1.1.2. Delito informático



Se denomina delito informático a aquella acción ilícita realizada por medio de Internet o que tiene como objetivo destruir o dañar ordenadores o redes de Internet.

Debido a que la informática avanza más rápido que la legislación, algunas conductas criminales por vías informáticas no pueden considerarse como delito y se definen como abusos informáticos.

Ejemplos de delitos informáticos: sabotaje informático, piratería informática, robo de identidad, ...

1.1.3. Hackear, crackear y hacking ético

Hackear: acción de entrar de manera forzada en un sistema informático o en una red. Puede referirse al robo de una contraseña, a la copia ilegal de un software protegido o a una acción que bloquee una página web.

Crackear: acción de modificar un programa con la finalidad de modificar su comportamiento original, generalmente para poder copiarlo o desprotegerlo.

Hacking ético: acción de realizar pruebas en redes para encontrar vulnerabilidades, sin hacer daño. El objetivo es encontrar, en una red, los elementos que son vulnerables y corregirlos antes de que se produzca un ataque.

1.1.4. Tipos de amenazas para los datos

Por su origen, podemos dividir las amenazas en cinco tipos:

- **Amenazas humanas:** Las personas son la principal amenaza para los sistemas de información. El objetivo puede ser muy variado:
 - Robo: sustracción de información, de equipos o de componentes de hardware.
 - Curiosidad: entrada al sistema, sin estar autorizado, por simple curiosidad o por desafío personal. Aunque no haya intención maliciosa, es peligrosa porque puede causar daños no intencionados.
 - Venganza: entrada al sistema de un ex empleado de una empresa (o un empleado con autorización) con la intención de extraer información o causar daño al sistema.
 - Terrorismo.
 - Sabotaje: entrada al sistema para interrumpir sus servicios o causar su destrucción completa.
 - Fraude: obtener beneficios ajenos a los objetivos de la organización.
 - Ingeniería social: obtener información confidencial a través de la manipulación de usuarios haciéndoles revelar información sensible.
- **Amenazas de hardware:** Fallos físicos por defectos de fabricación, mal diseño del hardware, fallos en el suministro eléctrico, mal uso o mal mantenimiento.
- **Amenazas de software:** Fallos del software del equipo por un mal diseño, mala implantación o por ataques de software externo como, por ejemplo, los virus.

- **Amenazas de red:** No disponibilidad de la red o extracción de información a través de la red provocada por un error físico o lógico del sistema o por un ataque deliberado.
- **Amenazas por desastres naturales:** los desastres naturales que amenazan a un sistema de información son muy variados: inundaciones, terremotos, incendios, huracanes, tormentas eléctricas, ... Pueden provocar la destrucción total o parcial de los equipos.

1.2. VALOR DE LA INFORMACIÓN

1.2.1. Motivos para proteger la información personal y la comercialmente delicada

Actualmente, uno de los principales activos de cualquier empresa es la información contenida en sus sistemas informáticos. Esta información puede perderse, deteriorarse, ser revelada a la competencia o robada. Esta pérdida puede paralizar la actividad de la empresa temporalmente y, en el peor de los casos, puede provocar la ruina de la empresa. En el caso de un usuario particular, la pérdida de su información puede tener consecuencias profesionales y, sobretodo, sentimentales.

Lo primero que tenemos que hacer para evitar la pérdida de nuestra información es hacer copias de seguridad lo más a menudo posible. Pero no basta con hacer copias de seguridad sino que también es necesario mantener dichas copias en un lugar distinto al que se encuentra el sistema informático que contiene la información. De este modo, se reduce el riesgo por catástrofes naturales o robos.

Gran parte de la información que se puede encontrar sobre nosotros en Internet la hemos compartido nosotros mismos: redes sociales, mensajería instantánea, blogs, foros, ... Cuanta más información se sepa de nosotros, más fácil lo tendrán aquellos que quieran hacer un uso indebido de ella. Pero no sólo debemos ser cuidadosos con lo que publicamos sobre nosotros, también debemos proteger la privacidad de nuestros amigos y familiares.

Es importante tener mucho cuidado al hacer públicos ciertos datos:

- **Datos personales:** El DNI o pasaporte no debemos facilitarlos sin más en Internet. Pueden usarlos para cometer fraudes suplantando nuestra identidad.
- **Correo electrónico:** Si nuestro correo deja de ser privado, comenzaremos a recibir cada vez más correo spam, mensajes con intentos de engaño (phishing), ...
- **Datos bancarios:** Facilitarlos nos puede exponer a una pérdida económica. Hay que ser precavido con las páginas web de compras online y nunca facilitarlos por correo electrónico.
- **Ubicación geográfica:** Publicar nuestra dirección o los lugares que solemos frecuentar permite que nos localicen o puedan conocer nuestra rutina. Podemos poner en riesgo nuestra seguridad y la de los nuestros.
- **Fotografías y vídeos:** Nuestras fotografías y vídeos personales contienen más información de la que pensamos: ubicaciones, quiénes son nuestros amigos y familiares, nivel económico, datos de nuestro domicilio, gustos, ...

1.2.2. Medidas para evitar el acceso no autorizado a datos

Son muchas las buenas prácticas que nos ayudarán a estar más seguros. Os exponemos algunas:

- **Usar contraseñas:** Usar contraseñas en todos los equipos utilizados, cambiarlas cada cierto tiempo y usar contraseñas largas, complicadas, con números y letras. También es conveniente utilizar distintas contraseñas para diferentes sitios.
- **Bloquear el ordenador:** Si te alejas de tu ordenador para descansar y no quieres apagarlo, bloquéalo para que solicite la contraseña si alguien intenta utilizarlo.
- **Activar un cortafuegos (firewall):** un cortafuegos por hardware protegerá todas los ordenadores conectados a la red. Un cortafuegos por software protegerá sólo el ordenador donde se instala. Antes de instalar un cortafuegos por software, comprueba si ya lo tienes instalado; normalmente, los programas antivirus ya vienen con un cortafuegos incluido.
- **Instalar antivirus:** es indispensable tener instalado un programa antivirus o un programa de protección contra programas espías.
- **Encriptar el disco duro:** la información que se guarda en el dispositivo estará protegida. Las últimas versiones de Windows, Mac, iOS y Android tienen formas de encriptar la información y lo único que se necesita es activarlo.
- **Equipo no conectado a Internet:** Para datos delicados o muy privados, una buena alternativa es guardarlos en un equipo que no se conecte a Internet.
- **No usar Wi-Fi pública:** Evitar realizar compras o transferencias electrónicas con este tipo de conexiones.
- **No abusar de la nube:** Evitar el almacenamiento de información delicada en internet.
- **Usar páginas "https"** (protocolo seguro de transferencia de hipertexto): Antes de dar cualquier dato personal en una página web, comprobad que tenga este protocolo mirando su dirección.
- **No aceptar cookies:** Programad el navegador para que no las acepte o no las aceptéis cuando entréis en páginas que nos lo piden.
- **Desactivar JavaScript:** en el navegador: Podéis descargar programas que lo bloquean.
- **Vigilar con el correo electrónico:** Abrir los archivos adjuntos de un correo electrónico sólo si se confía en quien lo envió. Ignorar los correos electrónicos con suplantación de identidad (se hacen pasar, por ejemplo, por tu banco y te piden información privada y confidencial).
- **Encriptar Chats y correos electrónicos:** en la red encontraréis muchos sistemas; los más seguros son: Gnu Privacy Guard (GPG), Pretty Good Privacy (PGP) y Thunderbird. Para proteger chats podéis usar OTR, un programa que encripta los mensajes y puede utilizarse, por ejemplo, con Google Hangout y Facebook.
- **Proteger teléfonos móviles:** Existen dispositivos para proteger las conversaciones de los móviles.

Algunas de estas prácticas pueden acarrear inconvenientes o pueden ser costosas. Habrá que sopesar los pros y los contras.

1.2.3. Características básicas de seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad, integridad y autenticación de la misma:

- **Confidencialidad:** impide la divulgación de información a personas o sistemas no autorizados.
- **Integridad:** busca mantener los datos libres de modificaciones no autorizadas.
- **Disponibilidad:** es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- **Autenticidad:** permite identificar el generador de la información.

1.2.4. Requisitos de protección, almacenamiento y control de datos/privacidad en el país

El tratamiento de los datos de carácter personal que reciba una empresa debe ajustarse a los principios y obligaciones establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Esta Ley Orgánica española tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Fue aprobada en las Cortes españolas el 13 de diciembre de 1999. Esta ley se desarrolla fundamentándose en el artículo 18 de la constitución española de 1978, sobre el derecho a la intimidad familiar y personal y el secreto de las comunicaciones.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

Esta ley afecta a todos los datos que hacen referencia a personas físicas registradas sobre cualquier soporte, informático o no. Quedan excluidas de esta normativa aquellos datos recogidos para uso doméstico, las materias clasificadas del Estado y aquellos ficheros que recogen datos sobre Terrorismo y otras formas de delincuencia organizada (no simple delincuencia).

A partir de esta ley se creó la Agencia Española de Protección de Datos, de ámbito estatal que vela por el cumplimiento de esta normativa. Podéis consultar vuestros derechos en su web:

<https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/index-ides-idphp.php>

1.3. SEGURIDAD PERSONAL

1.3.1. Ingeniería social: phishing, shoulder surfing, ...

La **Ingeniería social** es la manipulación de usuarios para obtener información confidencial que permita realizar algún acto que perjudique o exponga la persona u organismo a riesgos o abusos.

La pesca electrónica o **phishing** es una de las diferentes técnicas utilizadas (lo comentaremos en el apartado 5.1.4.).

El **shoulder surfing** es una de las técnicas más viejas para la obtención de información confidencial. Su uso es tan sencillo como acercarse silenciosamente por la espalda de alguien y observar las teclas, el monitor o cualquier otro soporte de información que pueda ser de interés. Para evitar este ataque existen medidas como el uso del carácter asterisco mientras se teclea una contraseña o los filtros de privacidad para los monitores.

1.3.2. Robo de identidad

El robo de identidad es la apropiación de los datos personales de un individuo para realizar todo tipo de operaciones, fingiendo ser la persona a la que se extrajo su información sensible. Se trata de un delito de estafa. Si alguien que, por su empleo tiene acceso a datos personales de otros, los da a conocer estará cometiendo un delito de revelación de secreto profesional.

Existen varios métodos para obtener datos de información personal:

- **Correos falsos:** el delincuente nos envía un correo haciéndose pasar por una organización, banco o empresa verdaderas pidiéndonos información que le permita acceder a algún recurso que utilicemos en esa organización, banco o empresa. A este procedimiento también se le conoce como *pretextar*.
- **Personal:** el delincuente obtiene información que le garantice acceso a algún recurso valioso simplemente escuchando o mirando.
- **Ataque organizado:** el delincuente intenta superar la seguridad de un banco, empresa u organización para obtener información personal de los clientes y luego acceder a algún recurso de esa empresa.
- **Ataque a servidores de almacenamiento de información online:** el delincuente intenta obtener datos de un servidor de datos en la nube; obteniendo contraseñas, DNI, cuentas bancarias, ...

1.4. SEGURIDAD DE UN ARCHIVO

1.4.1. Macros

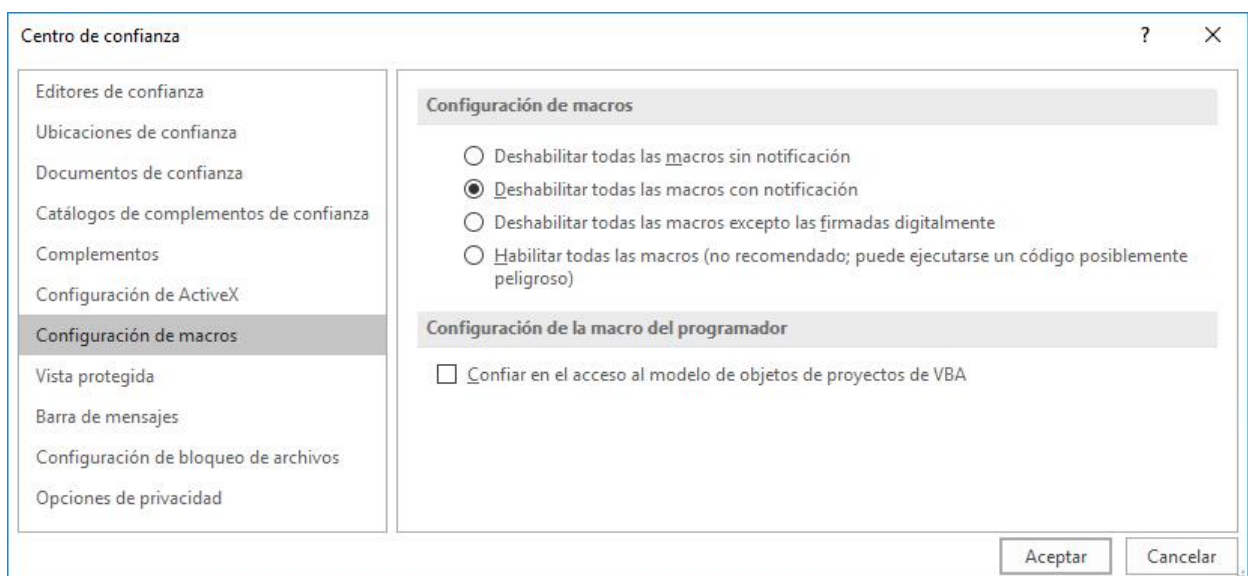
Las macros son un grupo de instrucciones que podemos programar para economizar tareas. Aplicaciones como Word, Excel o Access nos permiten crear macros que se ejecutarán automáticamente o cuando las llame el usuario. Por ejemplo, en Access podemos crear una macro que, al abrir la base de datos, muestre un determinado formulario o una macro que, al llamarla, abra un informe y lo imprima. Crear una macro nos permite ahorrarnos aquellas tareas que tenemos que hacer a menudo.

Las macros se pueden crear de dos maneras:

- Con la **grabadora de macros**: La grabadora de macros se limita a grabar cosas repetitivas que se hacen con el teclado y el ratón y no requiere conocimientos de programación, cualquier usuario las puede crear.
- **Escribiendo los códigos en el Editor de VBA**: Esta opción es más potente pero requiere conocimientos de programación (VBA: Visual Basic for Applications).

Dado que normalmente pensamos que los virus no vienen en documentos, sólo en archivos ejecutables, los ciberdelincuentes añaden macros maliciosas a los documentos para aprovechar nuestra confianza. Si abrimos un archivo que contenga una macro maliciosa podemos causar algún tipo de daño al equipo. Por eso, de manera predeterminada, las aplicaciones no permiten ejecutar macros automáticamente. El problema es que si el documento tiene macros no maliciosas, también quedan bloqueadas. Esta protección la podemos desactivar siguiendo los siguientes pasos (para Office 2010, 2013 y 2016):

1. En la ficha **Archivo** (para **Office 2010, 2013 y 2016**) seleccionamos la opción **Opciones**. En **Office 2007** la encontraremos en el **Botón de Microsoft Office**. En **Office 2003** la encontraremos en el menú **Herramientas**.
2. Hacemos clic en el botón **Configuración del centro de confianza** del apartado **Centro de confianza**.



3. Seleccionamos la opción que nos interese:

- **Deshabilitar todas las macros sin notificación:** Deshabilita las macros y permite ejecutar sólo las que se han guardado en un lugar de confianza. Los lugares de confianza se configuran en el apartado **Ubicaciones de confianza** de este cuadro de diálogo.
- **Deshabilitar todas las macros con notificación:** Muestra una alerta de seguridad advirtiendo sobre la intención de ejecutar una macro de manera que se pueda decidir si se desea ejecutar. Es la opción predeterminada.
- **Deshabilitar todas las macros excepto las firmadas digitalmente:** Sólo se podrán ejecutar las macros que estén firmadas digitalmente.
- **Habilitar todas las macros:** Permite ejecutar todas las macros sin enviar notificación al usuario. Esta opción es útil si se ejecutan múltiples macros confiables. Esta opción nos deja desprotegidos ante las maliciosas.

A partir de Office 2010, al abrir un documento que no está en nuestro disco duro, el documento se abre bloqueado; podemos mirarlo e imprimirlo pero no podemos modificarlo. Se trata de una protección que evita que se ejecuten las macros; si consideramos que no hay ningún peligro; sólo hay que clicar el botón **Habilita** que aparece en la parte superior de la ventana para editar el documento. Si el documento contiene una macro maliciosa, se activará.

1.4.2. Establecer una contraseña

Las contraseñas son nuestra primera línea de defensa contra el acceso no autorizado al equipo. Cuanto más segura sea la contraseña (más difícil de adivinar o descifrar), más protegido estará el equipo. Cada vez nos encontramos con más servicios que nos exigen una contraseña segura.

Recomendaciones para crear una contraseña segura:

- Ha de tener ocho caracteres, como mínimo.
- No debe contener datos personales o de la empresa.
- No debe contener una palabra completa.
- Debe ser significativamente diferente de otras contraseñas anteriores.
- Debe contener diferentes tipos de caracteres: letras mayúsculas y letras minúsculas, números y símbolos (! @ # \$ % ^ & * () _ ...).



El problema de las contraseñas seguras es que son difíciles de recordar. Hay que echarle imaginación para encontrar una combinación que nos sea fácil de recordar. Lo ideal es utilizar contraseñas diferentes para equipos o sitios diferentes. Por la dificultad que todo lo que hemos dicho provoca a la hora de recordarlas, es conveniente anotarlas en algún sitio. Nunca las anotéis en el mismo equipo y hacerlo de manera que, si alguien las encuentra, no sepa que son contraseñas o, al menos, que no sepa dónde utilizarlas. Otra técnica muy útil es cambiarlas a menudo aunque esto nos supondrá un esfuerzo de memorización.

1.4.3. Cifrado

El cifrado es un método que permite **aumentar la seguridad de un mensaje o de un archivo** mediante la codificación de su contenido. El cifrado no impide que alguien pueda ver el mensaje o el archivo pero evitará que pueda leerlo de no ser que disponga de la clave de cifrado para descodificarlo.

Por ejemplo, si realizamos una compra en un sitio web protegido (con protocolo https) la información de la transacción (dirección, teléfono número de tarjeta de crédito,...) se envía cifrada; aunque alguien la intercepte, no podrá leerla.

El cifrado también tiene **inconvenientes**. El más obvio es que si perdemos la clave usada al cifrar, perdemos el acceso al archivo. Otro inconveniente del cifrado es la lentitud, coste e incomodidad que supone el uso de técnicas de cifrado fuertes, aunque estos inconvenientes se van solucionando.

Hasta no hace mucho, el cifrado sólo estaba al alcance de gobiernos y grandes empresas. Ahora cualquiera puede usar las técnicas de cifrado más potentes en su ordenador personal o teléfono móvil.

Hay dos situaciones en las que nos puede interesar usar el cifrado; según sea el caso, podemos utilizar diferentes aplicaciones:

- **Cifrado en tránsito:** asegurar la privacidad de tus datos mientras son transmitidos por la red.

Aplicaciones:

- HotSpot Shield, un túnel VPN que protege la conexión frente a escuchas.
- BoxCryptor, que cifra archivos de Dropbox y otras nubes.
- PGP, muy usado para cifrar correos electrónicos (o GnuPG).
- TigerChat y otras apps de mensajería segura.

- **Cifrado local:** asegurar la privacidad de vuestros archivos.

Aplicaciones:

- TrueCrypt, una utilidad que crea unidades cifradas virtuales.
- FreeOTFE, una excelente alternativa a TrueCrypt.
- AxCrypt, una suite de cifrado para Windows.
- SSE, una suite de cifrado para móviles Android.

Windows permite **cifrar** carpetas o archivos sin necesidad de ninguna aplicación:

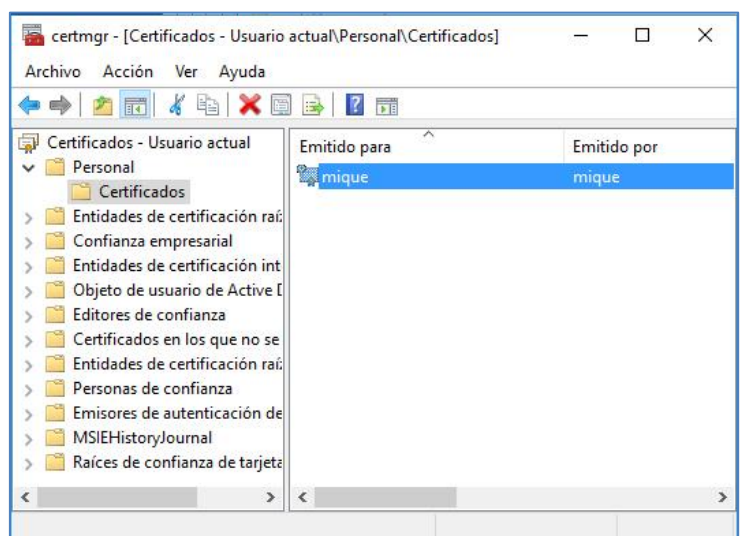
- Haced clic, con el botón derecho del ratón, en la carpeta o archivo que deseéis cifrar y escoged la opción **Propiedades**.
- En la ficha **General** clicad el botón **Opciones avanzadas**.
- Activad la opción **Cifrar contenido para proteger datos**.


Para **descifrar** una carpeta o un archivo:

- Haced clic, con el botón derecho del ratón, en la carpeta o archivo que deseéis descifrar y escoged la opción **Propiedades**.
- En la ficha **General** clicad el botón **Opciones avanzadas**.
- Desactivad la opción **Cifrar contenido para proteger datos**.

Si la clave de cifrado se pierde o queda dañada, los datos se perderán. Para asegurarse de tener siempre acceso a los datos cifrados, hay que hacer una **copia de seguridad de la clave y del certificado de cifrado**:

- Escribid *certmgr.msc* en el Campo de Búsquedas (Botón **Inicio**) y, cuando lo encuentre, abridlo. Si pide la contraseña de administrador o confirmación, escribid la contraseña o dad la confirmación.
- En el panel izquierdo, haced doble clic en **Personal** y después haced clic en **Certificados**.
- Seleccionad todos los certificados que haya en el panel de la derecha.
- En el menú **Acción**, escoged **Exportar** en la opción **Todas las tareas**.



El proceso anterior os lo podéis ahorrar si aparece, en la **barra de Tareas**, el icono . Hacedle un clic. Os preguntará si queréis hacer la copia de seguridad: Escoged **Hacer copia de seguridad ahora (recomendado)**. Haced los pasos anteriores sólo si no localizáis el icono.

- Se activará el Asistente para exportación de certificados. Haced clic en **Siguiente** en la primera pantalla.
- En la segunda pantalla, activad la opción **Exportar la clave privada**.
- En la tercera pantalla, seleccionad el formato (podéis dejar el que marca por defecto).
- En la cuarta pantalla, escribid la contraseña.
- En la quinta pantalla, escribid un nombre para el archivo donde guardará la copia de seguridad. Si no especificáis una ubicación (botón **Examinar**), lo guardará en la carpeta System32 de la carpeta Windows, en la unidad C:.
- En la última pantalla, haced clic en **Finalizar**.

Guardad el archivo creado (es la copia de seguridad del certificado EFS) en un lugar seguro.

1.4.4. Compresión de archivos

Una manera sencilla aunque que no muy segura de proteger un archivo es comprimirlo asignándole una contraseña. Hay diferentes aplicaciones que hacen esta tarea (7-Zip, WinRAR,...) y todas tienen un funcionamiento similar.

Lo más práctico es usar la herramienta de compresión de Windows 10; para comprimir un archivo o carpeta sólo hay que seleccionarlo, (botón derecho del ratón) y escoger la opción **Enviar a - Carpeta comprimida (en zip)**. Creará un archivo en el mismo directorio, con el mismo nombre y con un icono de carpeta con cremallera.



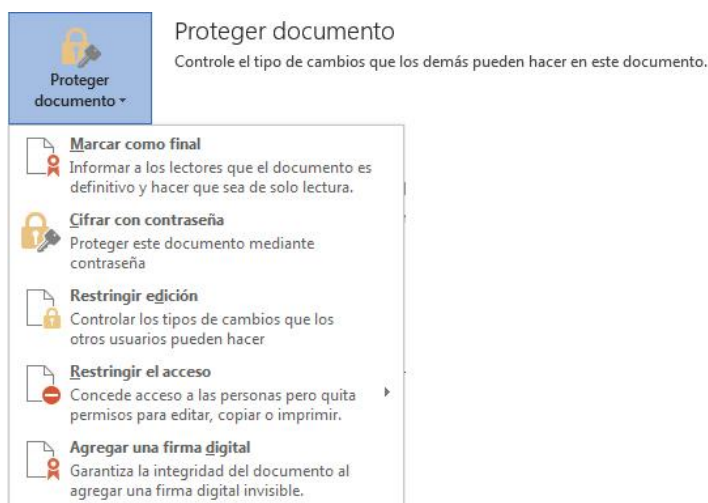
Si utilizáis aplicaciones de compresión tendréis la ventaja de poder especificar el grado de compresión y la posibilidad de ponerle una contraseña de acceso.

Para **descomprimir**, seleccionad el archivo que queréis descomprimir y, con el botón derecho del ratón, pedís la opción **Extraer todo....**

Haciéndole un doble clic podéis abrir el archivo sin descomprimirlo. Cuando lo cerréis, continuará comprimido.

1.4.5. Proteger un archivo con su aplicación

La mayoría de aplicaciones permiten cifrar, asignar una clave de acceso a sus archivos y restringir la edición. Por ejemplo, en Microsoft Word tenéis, en la ficha **Archivo (Información)**, el botón **Proteger documento**.



1.4.6. Keyloggers

Las contraseñas y cifrados son vulnerables a los ataques de los keyloggers. Un keylogger es un software o un hardware que se encarga de registrar las pulsaciones que se realizan en el teclado para memorizarlas en un archivo o enviarlas a través de Internet. Se usan para tener acceso a contraseñas, número de la tarjeta de crédito,...

2. MALWARE

2.1. DEFINICIÓN, FUNCIÓN Y TIPOS

Malware (**malicious software**) o **software malicioso** es el software que tiene como objetivo infiltrarse o dañar un ordenador o sistema de información sin el consentimiento de su propietario. Normalmente usamos, incorrectamente, el término virus informático para referirnos a este tipo de software; los virus son uno de los diferentes tipos de malware.

Los primeros malware fueron creados como experimentos o bromas, no para causar daños. En la actualidad, algunos son diseñados para destruir archivos en el disco duro o para corromper el sistema de archivos escribiendo datos inválidos. Otros son diseñados para atacar páginas web y dejar una huella como ocurre con el grafiti.

Con el aumento de usuarios de Internet, este software malicioso ha empezado a utilizarse para sacar beneficio, legal o ilegalmente. Desde 2003, la mayor parte han sido diseñados para tomar el control de ordenadores para su explotación en el mercado negro. Estos ordenadores infectados “ordenadores zombis” son usados, por ejemplo, para el envío masivo de spam o para alojar datos ilegales como pornografía infantil.

Muchos se utilizan para mostrar publicidad no deseada o redireccionar visitas hacia publicidad para beneficio del creador. Estos tipos de malware no se propagan como los virus, generalmente son instalados aprovechándose de vulnerabilidades o junto con software legítimo.

Existen muchos **tipos de malware**; veremos los más importantes:

- **Virus informáticos:** usan diferentes portadores pero los más comunes son los archivos ejecutables, que pueden ser parte de las aplicaciones, los documentos que contienen macros y los sectores de arrancada de los discos. El contagio se produce al pasar el archivo de un ordenador a otro.
- **Gusanos:** son similares a los virus, pero no dependen de archivos portadores para contaminar otros sistemas. Pueden modificar el sistema operativo con el objetivo de autoejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, explotan vulnerabilidades del objetivo o usan algún mecanismo de ingeniería social para engañar a los usuarios y poder ejecutarse.
- **Troyano informático:** es un programa nocivo con apariencia de programa legítimo. Los troyanos no son capaces de replicarse por ellos mismos y pueden ser adjuntados con cualquier tipo de software o pueden introducirse por medio del engaño.
- **Backdoor** (puerta trasera): es un programa que permite el acceso al ordenador ignorando los procedimientos normales de autenticación. Según cómo trabajen e infecten otros equipos, hay dos tipos:
 - Los que se parecen a los troyanos, es decir, son insertados manualmente dentro de otro programa, ejecutados por el programa contaminante e infectan al sistema para ser instalados permanentemente.

- Los que funcionan de forma parecida a un gusano informático, que se ejecuta como un procedimiento de inicialización del sistema y normalmente infecta mediante gusanos que lo llevan como carga.
- **Spyware** (Software espía): es aquel software que recolecta y envía información de los usuarios. Normalmente trabajan y contaminan sistemas como lo hacen los troyanos.
- **Exploit**: es aquel software que ataca una vulnerabilidad particular de un sistema operativo. No son necesariamente nocivos, son generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad.
- **Rootkit** (herramienta de intrusión): es un software que permite un acceso de privilegio continuo a un ordenador pero que mantiene su presencia oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de aplicaciones. Permite al atacante tomar el control del sistema y ocultar otro malware.
- **Ransomware**: es un software que restringe el acceso a los archivos de un ordenador de forma ilícita y exige un rescate económico para retirar las restricciones. El método más habitual es la codificación con una clave secreta que sólo conocen los atacantes.

2.2. PROTECCIÓN

Para prevenir los ataques a nuestro ordenador es indispensable tener un antivirus actualizado que minimice el riesgo. El software antivirus es un programa que detecta, previene y toma medidas para desarmar o eliminar malware, como virus y gusanos.

2.2.1. Cómo funciona un virus

Un **virus** tiene un proceso de creación, contagio, incubación, replicación y ataque:

- **Creación**: El virus se crea como subprograma o microprograma ejecutable. Después se suelta en la Red o se copia dentro de un programa comercial de gran difusión, para asegurar un contagio rápido y masivo. A partir de aquí, el virus actúa de forma automática e independiente del control de su creador.
- **Contagio**: Es, quizás, la fase más fácil de todo el proceso. Sólo hay que tener en cuenta que el virus debe introducirse o soltarse en la Red. El virus debe ir incrustado en un archivo de instalación o en una simple página Web a través de las *cookies*. Las vías de infección son también principalmente los programas copiados, Internet o el propio correo electrónico.
- **Incubación**: Normalmente los virus se crean de formas específicas que atienden a una serie de instrucciones programadas como el esconderse y reproducirse mientras se cumplen unas determinadas opciones predeterminadas por el creador del virus. Así, el virus permanece escondido reproduciéndose en espera de

activarse cuando se cumplan las condiciones. Este proceso puede ser muy rápido en algunos casos y bastante largo en otros, según el tipo de virus.

- **Replicación:** Consiste en la producción del propio virus de una copia de sí mismo, que se situará en otro archivo. De esta forma, el virus se contagia en otros archivos y otros programas, asegurándose de que el proceso de multiplicación está asegurado. Además, el virus asegura su extensión a otros ordenadores y debe hacerlo de la forma más discreta y rápida posible. En este momento, el virus no se manifiesta, ya que sólo se instala en el mayor número de lugares posible. Sólo de esta forma tendrá más posibilidades de dañar a una cantidad mayor de ordenadores.
- **Ataque:** Cuando se cumplen las condiciones, el virus entra en actividad destructora. Aquí es donde, por ejemplo, formatea el disco duro o borra archivos con una determinada extensión. El ataque es el escalón final del trabajo del virus; el ordenador se encuentra infectado y, si no se dispone de un programa que elimine el virus, jamás se podrán recuperar los archivos. Podemos instalar de nuevo el software, pero nuevamente se activará la destrucción en el momento que se cumplan las condiciones.

Para la propagación del virus, a veces, el atacante utiliza una **botnet**: grupo de ordenadores conectados a Internet (llamados zombies) que, involuntariamente, una vez infectados son controlados remotamente sin que el propietario se dé cuenta.

2.2.2. Síntomas que indican la presencia de virus informáticos

¿Cómo sabemos que nuestro ordenador está infectado? Es difícil, pero hay ciertos síntomas que delatan la posible presencia de virus, aunque también podrían deberse a otros problemas ajenos a los virus:

- Sin causa aparente, se hace más lento el trabajo del ordenador o se queda colgado demasiado a menudo.
- El disco duro trabaja más de lo habitual. Esto se ve desde el indicador led del disco duro que parpadea cuando estamos inactivos.
- El sistema no arranca o se reinicia solo.
- Algunos programas no pueden ejecutarse.
- Se reduce el espacio disponible en los discos.
- El sistema no reconoce alguna unidad de disco.
- Se reduce la memoria disponible.
- Aparecen en la pantalla mensajes extraños o de aviso, que nada tienen que ver con los habituales mensajes de Windows.
- La pantalla se borra o cambia.
- Aumenta el tamaño de los archivos o no los podemos abrir.
- Aparecen o desaparecen algunos archivos. Algunos aparecen con el mismo nombre que otros.
- En algunos ficheros aparece información de otros.

2.2.3. Cómo funciona un software de antivirus y sus limitaciones

Un antivirus es un programa que tiene tres **objetivos básicos**:

- Detectar la presencia de malware en los archivos.
- Desinfectar todos aquellos archivos que contengan virus.
- Proteger al ordenador frente a futuros ataques.

Un Antivirus **actúa** de la siguiente forma:

- Inspecciona todos los correos que se reciben en el ordenador y busca malware para eliminarlo.
- Monitoriza los archivos del ordenador a medida que van siendo abiertos o creados para garantizar que no estén infectados.
- Inspecciona periódicamente todo el ordenador para verificar si existen archivos corruptos y eliminar el malware existente.

Los antivirus utilizan una base de datos para localizar las amenazas. Por ello, es muy importante actualizarlos ya que, de no hacerlo, se volverán totalmente inútiles ya que no reconocerán las amenazas más recientes.

Aunque los antivirus cada vez ofrecen más funcionalidades, no son infalibles, tienen **limitaciones**. Por ejemplo:

- No evitan el Spam. Deberemos utilizar un software Anti-Spam específico.
- No evitan ataques directos de un hacker al ordenador.
- No evitan las actividades criminales online.

A pesar de las limitaciones, nunca hay que detener el funcionamiento del antivirus porque dejará al ordenador expuesto a ataques.

La mejor actitud para evitar los efectos de los virus es la prevención. Además de utilizar un antivirus actualizado, es conveniente no introducir a través de la red ficheros sospechosos y, sobre todo, tener cuidado con los archivos que se intercambian.

Aunque estéis tentados a utilizar más de un antivirus para aumentar la seguridad, no lo hagáis porque normalmente entran en conflicto entre ellos y podríais tener problemas.

2.2.4. Antivirus de pago y gratuitos

Existen en el mercado muchos programas antivirus, tanto de pago como gratuitos. Si queremos la máxima seguridad posible, mejor utilizar un antivirus de pago: Kaspersky, McAfee VirusScan, Norton, NOD32, Panda, Bitdefender, Avast, Trend Micro, ...

Si somos precavidos (sobre todo cuando navegamos por Internet), podemos utilizar antivirus gratuitos pero tenemos que tener presente que su efectividad será menor. Los fabricantes están muy interesados en vender licencias de sus paquetes completos, por lo que es lógico que las versiones gratuitas tengan limitaciones, suficientes para animar al usuario a adquirir una protección mayor.

Si optáis por el uso de un antivirus gratuito, a la hora de elegir tened en cuenta las desventajas de los antivirus gratuitos más conocidos:

- AVAST 7: Se ha hecho cada vez más lento pero es de los mejores. Si el ordenador es potente, no lo notaremos.
- AVG 2013: Se hace pesado con los mensajes donde nos pide registrarlo pero después no nos lo facilita.
- MICROSOFT SECURITY ESSENTIALS: La desactivación no es sencilla. Excelente integración en el sistema y menús, pero a diferencia de otros antivirus gratuitos, para desactivarlo temporalmente nos obliga a pasar por el panel de configuración.
- BITDEFENDER FREE: Aunque la edición gratuita es rápida y efectiva, no da apenas información en la web oficial y no hay versión en castellano. Al comprarlo sí dispondremos de todas las opciones en castellano.
- AVIRA 2013: La protección es muy reducida.

A pesar de estos inconvenientes, estos antivirus gratuitos son muy útiles, pero cada vez está más clara la función de “puentes” hacia ediciones de pago.

Estos comentarios los hacemos sobre las versiones que hay en el momento de redactar estos apuntes. Cuando lo leáis puede haber cambiado mucho.

2.2.5. Analizar unidades, carpetas y archivos específicos

En algún momento podemos querer analizar un determinado archivo, una unidad extraíble, un disco, una unidad o una carpeta de nuestro equipo porque sospechamos que puede contener malware. Podemos analizarlo sin necesidad de analizar el equipo completo; simplemente hay que hacer un clic, con el botón derecho del ratón, sobre el archivo, unidad extraíble, disco, unidad o carpeta que queremos analizar y, en el menú contextual que aparece, pedir la opción **Digitalizar con** o **Analizar con** seguida del nombre de vuestro antivirus. Dependiendo del antivirus, puede tener otro nombre pero siempre tiene el nombre del antivirus.

2.2.6. Cuarentena

La cuarentena es la acción que realizan los antivirus para impedir que un archivo, que está infectado con un virus, contagie al resto de archivos del ordenador, aislándolo de los demás.

Esta acción la realizan cuando no pueden eliminar el archivo infectado o cuando su eliminación puede poner en peligro al sistema. También podemos pedirla nosotros cuando detecta el archivo infectado y nos pregunta si queremos que lo elimine o que lo ponga en cuarentena.

El antivirus cifrará el archivo y lo moverá a una carpeta de cuarentena ubicada en la carpeta de instalación del programa. Una vez puesto en cuarentena podemos, nosotros, intentar eliminarlo manualmente o esperar a que una actualización del antivirus le permita eliminarlo.

3. SEGURIDAD DE LA RED

3.1. REDES

3.1.1. Conceptos

El entorno del ordenador personal se ha quedado pequeño para aquellos que cuentan con varios equipos en pequeñas o grandes oficinas o entornos de trabajo. La informática ofrece su propia solución: la red. Con ella es posible duplicar aplicaciones, impresoras y otros recursos.

La interconexión de ordenadores mediante los sistemas de telecomunicaciones han revolucionado el mundo de la informática y al mundo en general. Esta conexión es el origen de las Tecnologías de la Información.

La importancia de las redes radica principalmente en la capacidad de compartir recursos, es decir, utilizar impresoras que no están conectadas a nuestro ordenador, consultar bases de datos remotas, enviar y recibir ficheros y datos de los distintos departamentos de la empresa, coordinación y mensajería, sistemas de copias de seguridad automatizados, sistemas antivirus y seguridad, servidores de aplicaciones, etc. En el caso de que sólo tengamos un módem, desde cualquiera de los equipos podremos conectar a Internet usando ese único dispositivo, sin necesidad de tener instalado uno en cada equipo. Por tanto, compartir recursos y aplicaciones es la forma de trabajo más eficaz y rentable.

Dependiendo de si se deben recorrer distancias geográficas grandes (como unir ordenadores de dos edificios distantes, recorrer dos ciudades distintas, o un continente) o por el contrario se deben recorrer distancias cortas (como una habitación, un edificio, o un pequeño campus) las redes de interconexión son diferentes y se clasifican en dos grandes categorías, que son:

- **LAN** (Local Area Networks - redes de área local): Denominamos de esta manera a un sistema de conexión entre ordenadores, red, formada a partir de 3 ordenadores interconectados generalmente en la misma habitación o edificio. Por ejemplo los ordenadores de la Facultad de Ingeniería de una universidad es una LAN. Proporcionan la velocidad de conexión más alta entre ordenadores.
- **WAN** (Wide Area Networks - redes de área amplia): Proporcionan comunicación que cubre grandes distancias, es una red de gran alcance que interconecta pequeñas redes locales (LAN), generalmente estas interconexiones entre LANs se realizan con fibra óptica o sistemas de alta velocidad. Por ejemplo la red de una universidad que interconecta a todas las facultades es una WAN.

Cuando hablamos de una **VPN** (Virtual Private Network - red privada virtual) nos referimos a una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Por ejemplo, un profesor de una universidad, que está de viaje, puede conectarse al ordenador de su despacho desde el hotel donde se hospeda. Aunque parezca un enlace privado, en realidad se trata de una WAN.

3.1.2. Rol del administrador de la red

Los administradores de red son los que mantienen el hardware y software de la red. Esto incluye el despliegue, mantenimiento y monitoreo del engranaje de la red: switches, routers, cortafuegos, ...

Algunas funciones del administrador de red son:

- Diseño y seguridad de la red.
- Proporcionar soporte.
- Administrar las cuentas de usuario.
- Administrar el espacio en discos y mantener copias de seguridad.
- Asegurarse de que la red se utiliza eficientemente
- Asignar direcciones.
- Configuración de autenticación y autorización.
- Mantenimiento de los servidores, las instalaciones de red y los detectores de intrusos.

3.1.3. Firewall (servidor de seguridad)

Un cortafuegos (Firewall) es un elemento de hardware o software utilizado en una red de equipos informáticos para controlar las comunicaciones del ordenador, permitiéndolas o prohibiéndolas según lo que se determine. Permite evitar accesos no deseados. El firewall bloquea los hackers, virus y software espía de Internet antes de entrar en el equipo.



Ventajas:

- Protege de intrusiones: Evita que cualquiera pueda acceder a cualquier equipo de la red.
- Protege la información privada. Permite definir diferentes niveles de acceso a la información de manera que en una organización cada grupo de usuarios tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- Optimiza el acceso: Optimiza la comunicación entre los equipos de la red.

Limitaciones:

- No puede proteger de los ataques que se efectúen fuera de su punto de operación.
- No puede proteger de los traidores o espías corporativos. Por ejemplo, no puede evitar que un empleado autorizado copie y los entregue a la competencia.
- No puede proteger de los ataques de la ingeniería social.
- No puede proteger de los ataques de virus informáticos a través de archivos y software. La solución es instalar software antivirus en cada equipo.
- No puede proteger de los errores de seguridad de los servicios que se publiquen en Internet.

3.2. CONEXIONES DE RED

3.2.1. Tipos de conexión

Los tipos de conexiones a Internet y los dispositivos utilizados han ido evolucionando buscando, principalmente, aumentar la velocidad en la transferencia de datos porque cada vez es necesaria una mayor velocidad para acceder a los nuevos servicios que nos ofrece Internet: recursos interactivos, juegos, televisión, videoconferencias, ...

A continuación veremos algunos tipos de conexión a Internet:

- **Red Telefónica Conmutada (RTC):** También conocida como Red Telefónica Básica. Por ella circulan habitualmente las vibraciones de la voz, las cuales son traducidas en impulsos eléctricos que se transmiten a través de dos hilos de cobre. A este tipo de comunicación se denomina analógica. Para enviar datos es necesario hacer una conversión de la señal para que pueda viajar por la red telefónica en forma analógica convirtiéndose en digital al llegar al ordenador.

Para acceder a la Red sólo necesitaremos una línea de teléfono y un módem. El módem (acrónimo formado por el inicio de las palabras que indican su función: modular-demodular) se encarga de la conversión. Los módems pueden tener velocidades de **56 kbps** para transmitir y para recibir y pueden ser internos o externos.

La RTC nos permite acceder a la Red de forma barata pero muy lenta comparada con otros tipos. Fue la primera utilizada para conectarnos a Internet y tuvo su auge en los años 80 y 90.

- **Red Digital de Servicios Integrados (RDSI):** La conexión divide la línea telefónica en tres canales: dos portadores, por los que circula la información a la velocidad de 64 kbps, y un canal, de 16 kbps, que gestiona la conexión. Se pueden utilizar los dos canales portadores de manera independiente (es posible hablar por teléfono por uno de ellos y navegar por Internet simultáneamente), o bien utilizarlos de manera conjunta, lo que proporciona una velocidad de transmisión de **128 kbps**.

Requiere un operador de telecomunicaciones y una conexión especial, que permite una velocidad de conexión digital a 64 kbps en ambos sentidos. Para el ordenador necesitaremos una tarjeta RDSI.

- **Línea de Abonado Digital Asimétrica / Asymmetric Digital Subscriber Line (ADSL):** Usa el par de cobre de la línea telefónica normal y la convierte en una línea de alta velocidad estableciendo tres canales independientes sobre la línea telefónica estándar: dos canales de alta velocidad (uno de recepción de datos y otro de envío de datos) y un tercer canal para la comunicación de voz (servicio telefónico básico). Los dos canales de datos son asimétricos, es decir, no tienen la misma velocidad de transmisión de datos. El canal de recepción de datos tiene mayor velocidad que el canal de envío de datos. Esta asimetría permite alcanzar mayores velocidades en el sentido “red → usuario”, lo cual se adapta a los servicios de acceso a información ya que, normalmente, el volumen de información recibido es mucho mayor que el enviado. La velocidad de transmisión (**de 10 a 20 Mbps**) depende de la distancia del módem a la centralita (a partir de 3 km baja la velocidad).

El envío y recepción de los datos se establece desde el ordenador del usuario a través de un módem ADSL. Estos datos pasan por un filtro (splitter), que permite la utilización simultánea del servicio telefónico básico (RTC) y del servicio ADSL, es decir, podemos hablar por teléfono y, a la vez, navegar por Internet.

- **Cable:** Normalmente se utiliza el cable coaxial que es capaz de conseguir elevadas velocidades de transmisión (**hasta 100 Mbps**) pero, en lugar de establecer una conexión directa (punto a punto) con el proveedor de acceso, se utilizan conexiones multipunto (muchos usuarios comparten el mismo cable).

Algunas características de esta tecnología son:

- Cada nodo (punto de conexión a la Red) puede dar servicio a entre 500 y 2000 usuarios.
 - Para una calidad óptima de conexión la distancia entre nodo y usuario no puede superar los 500 m.
 - No se pueden utilizar los cables de las líneas telefónicas tradicionales, es necesario que el cable coaxial alcance físicamente el lugar desde el que se conecta el usuario.
 - La conexión es compartida, por lo que a medida que aumenta el número de usuarios conectados al mismo nodo, se reduce la tasa de transferencia de cada uno de ellos.
- **Vía satélite:** Este tipo de conexión permite aliviar la congestión existente en las redes terrestres tradicionales y disponer de conexión en lugares donde no llega la red terrestre.

Generalmente se emplea un híbrido de satélite y teléfono: se necesita una antena parabólica digital, un acceso telefónico a Internet, una tarjeta receptora para PC, un software específico y una suscripción a un proveedor de satélite. El usuario envía sus peticiones (consume muy poco ancho de banda) mediante un módem tradicional, pero la recepción (consume mucho) se produce por una parabólica. Velocidad de **hasta 1 Mbps**.

Otra variante es utilizar sólo satélite para enviar y recibir, permitiendo el acceso a Internet desde cualquier zona de cobertura del satélite. La velocidad de bajada es de **hasta 38 Mbps** y, la de subida, **hasta 2 Mbps**.

- **Wi-Fi:** No es un tipo de conexión a Internet pero sí que es uno de los medios de conexión a Internet más utilizados. La posibilidad de movilidad que ofrece este medio de conexión y su servicio gratuito en muchos lugares (principalmente públicos) hace que sea un servicio en auge. Podemos movernos por nuestra casa, centro educativo, trabajo, parques públicos... con nuestros portátiles, nettops, netbooks o teléfonos móviles teniendo conexión a Internet y sin necesidad de estar pendientes de un punto de acceso que nos limite nuestra movilidad.
- **Internet móvil: High Speed Downlink Packet Access (HSDPA):** La tecnología móvil es la que evoluciona con mayor rapidez. Hemos pasado rápidamente por etapas significadas por siglas que suponen un sucesivo avance de la tecnología: 1G, GSM, 2G, GPRS, EDGE, 3G, UMTS, WCDMA... hasta llegar al momento actual de HSDPA. Cuando leáis esto seguramente esta tecnología ya será historia.

La tecnología HSDPA permite alcanzar tasas de **hasta 14 Mbps**. Permite videoconferencia, juegos online multiusuarios, películas, vídeos, descargas y ejecución de programas,... todo en tiempo "real". Proporciona un

acceso a Internet de mayor ancho de banda, para una ejecución más rápida de los servicios y recursos, y posibilita que un mayor número de usuarios puedan utilizar simultáneamente la red.

Las operadoras de telefonía 3G utilizan esta tecnología y la dirigen principalmente al mercado móvil de los portátiles y los móviles 3G:


- **Ordenadores de pequeño tamaño:** portátiles, netops, netbooks,... conectados principalmente mediante un modem USB que incorpora una tarjeta SIM del operador telefónico que presta el servicio. La ventaja radica en la no dependencia de una conexión fija o Wi-Fi para conectar a Internet y de no perder la característica de movilidad que nos ofrecen los ordenadores portátiles. La configuración es instantánea al conectar el modem USB y teclear el número de activación (PIN) como si de un teléfono móvil se tratara. Dependiendo de las condiciones de cobertura y señal, la velocidad puede llegar **hasta 7,2 Mbps**.
- **Teléfonos móviles 3G:** No requiere ninguna instalación pues está integrado en el teléfono y las únicas limitaciones son las establecidas en su tipo de contrato y las posibilidades del propio modelo de terminal. Las velocidades normales de estos móviles 3G rondan los **3 Mbps / 1,4 Mbps** pudiéndose alcanzar velocidades mucho más elevadas en conexiones Wi-Fi.

3.2.2. Implicaciones para la seguridad

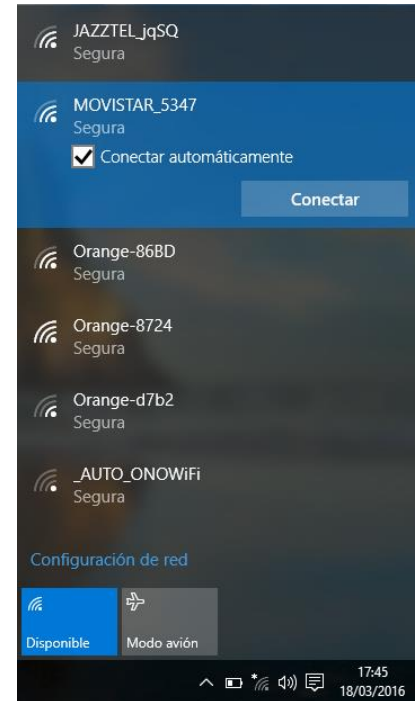
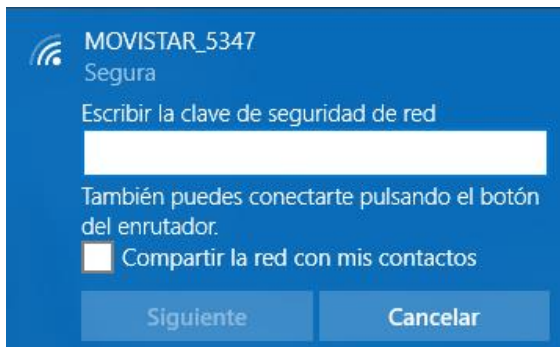
Conectar nuestro equipo a una red disminuye, lógicamente, su seguridad. Un equipo no conectado a una red, sólo está expuesto a ataques cuando le conectamos un dispositivo externo, como un USB, o le introducimos un disco, CD o DVD. Estas amenazas las podemos controlar con relativa facilidad pero, en el momento que conectamos nuestro equipo a la red, estamos expuestos a todo tipo de amenazas provenientes de cualquier parte. Estaremos expuestos a amenazas, como el acceso a nuestros datos, que sin conexión a red no existían. Por lo tanto, en el momento que un equipo lo conectamos a la red, debemos extremar las medidas de seguridad y ser más cautelosos.


3.3. SEGURIDAD INALÁMBRICA

3.3.1. Conectarse a una red inalámbrica

En **Windows 10**, el botón **Acceso a Internet** , situado a la derecha de la **Barra de Tareas**, muestra el panel de redes disponibles. Al seleccionar la red a la que queremos conectar-nos, aparecerá el botón **Conectar**; clicad este botón para iniciar la configuración del acceso a la red.

Pedirá la clave de la red que podéis ver en la parte inferior del router.

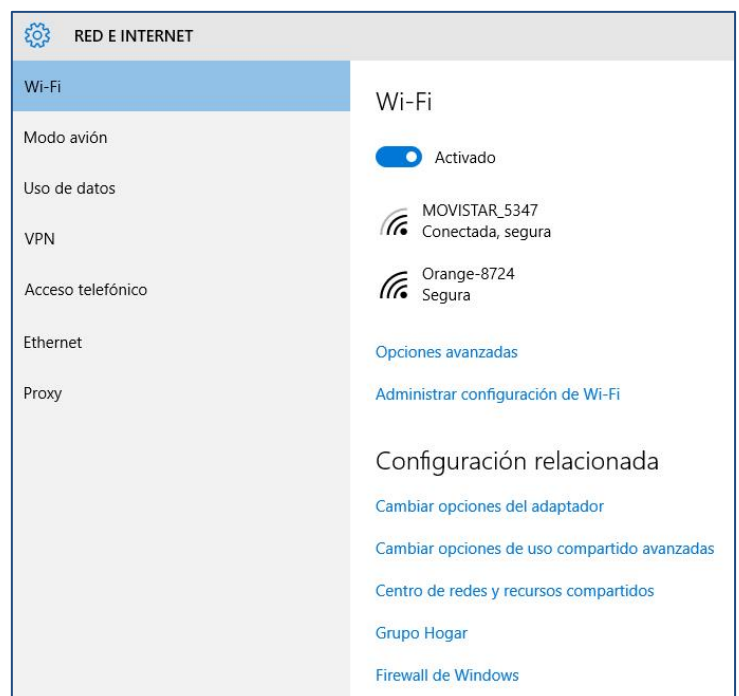


En **Windows 7** se hace igual; el icono es este: .

Una vez conectados a la red, al seleccionarla en la lista de redes disponibles, veremos que el botón **Conectar** ha sido substituido por el botón **Desconectar**. Si no la desconectamos, la próxima vez que encendamos el ordenador se conectará automáticamente a esta red, sin que tengamos que hacer nada.

Para cualquier otro tipo de configuración, usad el enlace **Configuración de red**:

En **Windows 7**, el enlace es **Abrir Centro de redes y recursos compartidos**. Os abrirá el **Panel de Control** correspondiente a la configuración de redes.



3.3.2. Proteger el acceso a una red inalámbrica

Una de las principales ventajas de la red inalámbrica es el ahorro en los costes de instalación ya que se elimina el cableado Ethernet y las conexiones físicas entre nodos, pero tiene una desventaja importante en cuanto a la seguridad. Con el cableado tenemos controlado quién se conecta a la red pero, con la red inalámbrica, sólo la clave de acceso impide el acceso a personas no autorizadas.

El acceso a nuestra red inalámbrica debe estar bien protegido y, para ello, lo mejor es utilizar un nombre de usuario y una buena clave de acceso para evitar el acceso de usuarios no autorizados.

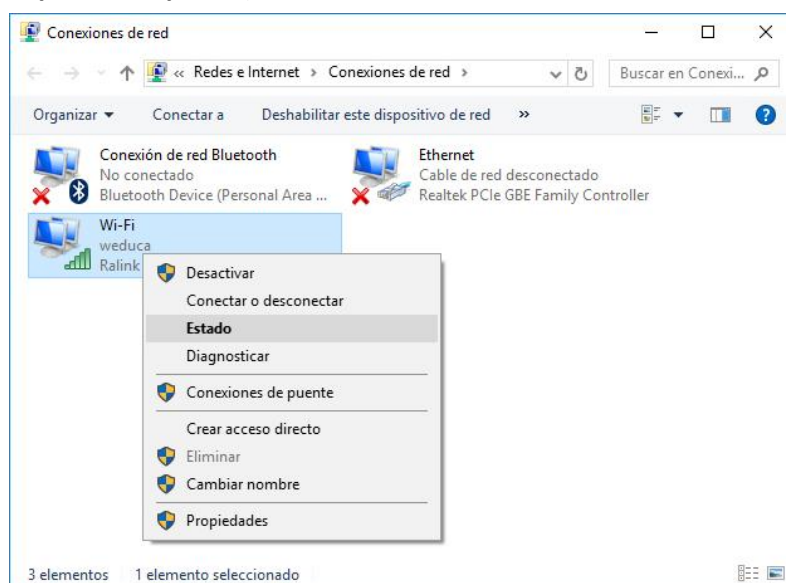
Al crear la clave evitad palabras fácilmente deducibles (nuestro nombre, el de la empresa, ...). Es aconsejable que tenga, al menos, 8 caracteres y combine letras y números. Hemos hablado de ello en el apartado 1.4.2.

En **Windows 10**, podéis **modificar la clave y el tipo de seguridad** de la vuestra red en el **Panel de Control** (lo encontraréis escribiendo *Panel de control* en el **Campo de Búsquedas**).

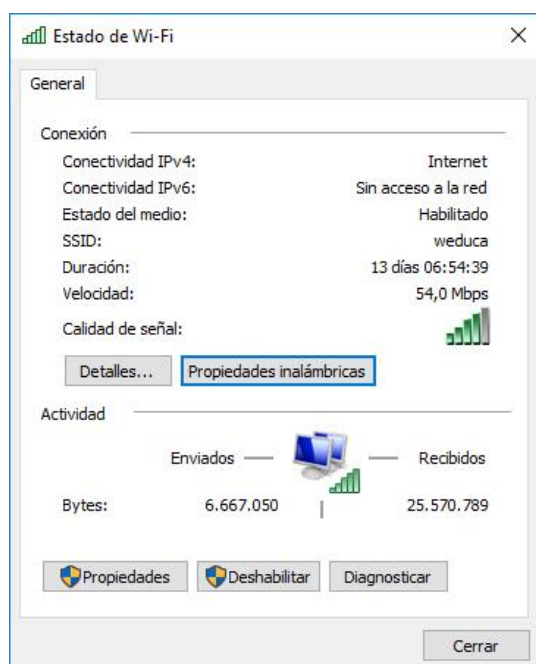
En la categoría **Redes e Internet**, escoged **Ver el estado y las tareas de red**.

En el panel de la izquierda, escoged **Cambiar configuración del adaptador**.

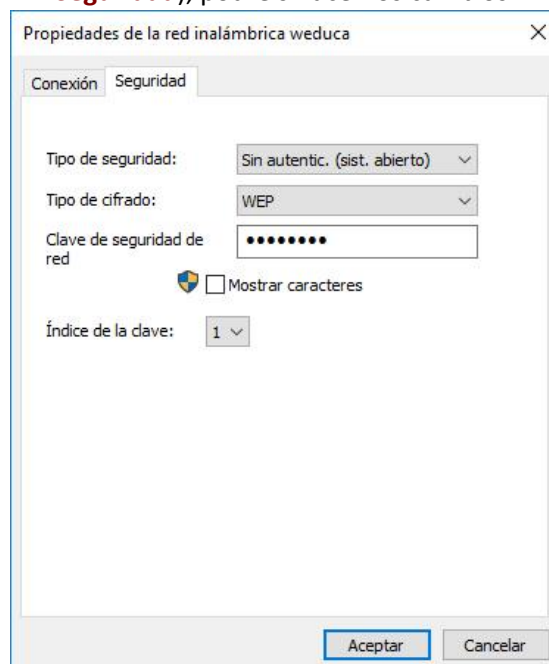
Clicad, con el botón derecho del ratón, sobre la red y escoged la opción **Estado**.




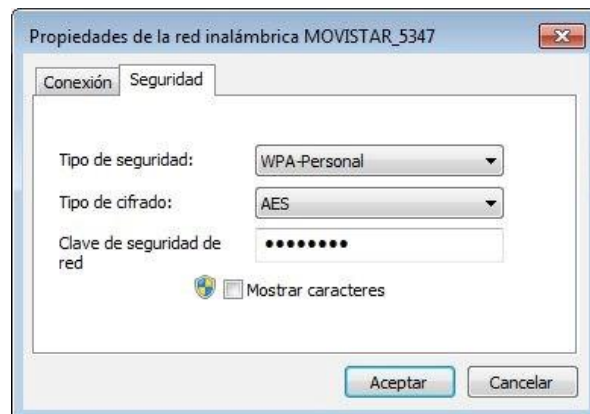
Clicad el botón **Propiedades inalámbricas**:



En el cuadro de diálogo que aparece (en la pestaña **Seguridad**), podréis hacer los cambios:



Para modificar la clave y el tipo de seguridad en **Windows 7**, abrid el panel con el botón **Acceso a Internet** () de la **Barra de Tareas**. Clicad, con el botón derecho del ratón, sobre vuestra conexión y escoged **Propiedades**. En el cuadro de diálogo que aparece, podréis hacer los cambios:



3.3.3. Tipos de seguridad inalámbrica

Por defecto, nuestra red inalámbrica está configurada con un determinado tipo de seguridad que, según el router, podremos modificar. Básicamente son estos:

- **Acceso protegido Wi-Fi (WPA y WPA2):** Cifra la información y se asegura de que la clave de seguridad de red no haya sido modificada. Además, autentifica a los usuarios con el fin de garantizar que únicamente las personas autorizadas puedan tener acceso a la red. Éste es el modo recomendado para redes domésticas.
Existen dos tipos de autenticación WPA: WPA y WPA2. WPA se ha diseñado para trabajar con todos los adaptadores de red inalámbricos, pero es posible que no funcione con enrutadores o puntos de acceso antiguos. WPA2 es más seguro que WPA, pero no funcionará con algunos adaptadores de red antiguos. WPA se ha diseñado para utilizarse con un servidor de autenticación 802.1x, que distribuye claves diferentes a cada usuario. Esto se denomina WPA-Enterprise o WPA2-Enterprise. También se puede usar en el modo de clave previamente compartida (PSK), donde cada usuario recibe la misma frase de contraseña. Esto se denomina WPA-Personal o WPA2-Personal.
- **Autenticación 802.1x:** La autenticación 802.1x puede ayudar a mejorar la seguridad de las redes inalámbricas 802.11 y de las redes Ethernet con cable. 802.1x usa un servidor de autenticación para validar a los usuarios y proporcionar acceso a la red. En las redes inalámbricas, 802.1x puede funcionar con claves WPA, WPA2 o WEP. Este tipo de configuración se utiliza en redes de trabajo.

Un método bastante seguro es indicar qué equipos pueden conectarse a la red. Para restringir el acceso, podemos utilizar el **Control de Acceso al Medio** - Media Access Control (**MAC**). MAC es el conjunto de mecanismos y protocolos de comunicaciones a través de los cuales varios interlocutores (ordenadores, teléfonos móviles, ...) se ponen de acuerdo para compartir un medio de transmisión común.

Algunas de sus funciones son:

- Controlar el acceso al medio físico de transmisión por parte de los dispositivos que comparten el mismo canal de comunicación.
- Agregar la dirección MAC del nodo fuente y del nodo destino en cada una de las tramas que se transmiten.
- Al transmitir en origen, debe delimitar las tramas de red agregando bits de bandera (flags) para que el receptor pueda reconocer el inicio y fin de cada trama.
- Al recibir en destino, debe determinar el inicio y el final de una trama de datos dentro de una cadena de bits recibidos por la capa física.
- Efectuar detección y, si procede, corrección de errores de transmisión.
- Descartar tramas duplicadas o erróneas.

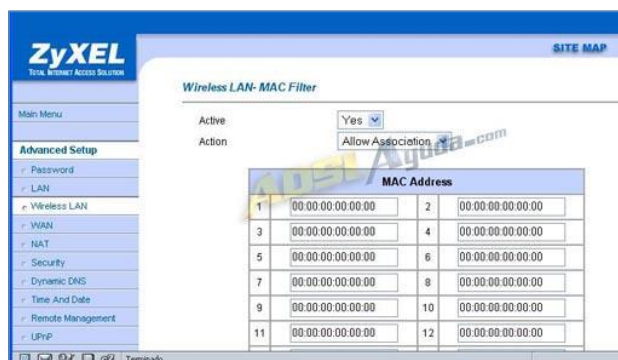
Cada tarjeta de red posee una dirección MAC única. Si queréis saber la vuestra, haced lo siguiente (en Windows):

Campo de Búsquedas - escribid **cmd** y, en la pantalla que aparece, escribid **ipconfig /all**

La dirección MAC la encontraréis en el apartado **Dirección física**.

El router WiFi por lo general permite crear una lista de direcciones MAC de las tarjetas de red que están autorizadas a conectarse a nuestra red y, así, evitar que otros equipos accedan a nuestra red. Es un filtro eficaz que también puede ser vulnerado pero con mayor dificultad. Para introducir las direcciones MAC de vuestros equipos haced lo siguiente:

- Desconectad vuestro router de la línea telefónica.
- Conectad vuestro router, con cable Ethernet, a vuestro ordenador.
- Abrid el navegador y escribid la IP de vuestro router.
- Aparecerá la página de configuración de vuestro router. Dependiendo del modelo será diferente pero lo que tenéis que hacer es buscar el apartado **Wireless LAN – MAC Filter**. Aquí escribiréis las direcciones MAC de vuestros equipos. Os ponemos, como ejemplo, la página de uno de los muchos modelos de router.



3.3.4. Riesgos de una red inalámbrica sin protección

La mayor amenaza para la seguridad de una red Wi-Fi gratuita es la capacidad del hacker de posicionarse entre el usuario y el punto de conexión. Por lo tanto, en lugar de comunicarnos directamente con el punto de conexión, estamos enviando la información al hacker, que después la transmite. Cuando se trabaja con esta configuración, el hacker tiene acceso a toda la información que se envía a través de Internet: correos electrónicos, información de tarjetas de crédito, contraseñas,...

Los hackers también pueden utilizar una conexión Wi-Fi no segura para distribuir malware. Si compartimos archivos a través de una red, el hacker puede introducir fácilmente software infectado. Algunos hacen que aparezca una ventana emergente durante el proceso de conexión que ofrece una actualización de un software conocido. Cuando se hace clic en la ventana, se instala el malware.

La gran mayoría de los hackers van simplemente tras objetivos fáciles, por lo que tomar unas cuantas precauciones debería mantener la seguridad de nuestra información:

- **Uso de una red privada virtual (VPN):** Es indispensable contar con una conexión de red privada virtual (VPN) cuando nos conectamos a nuestra empresa a través de una conexión no segura. Incluso si un hacker logra posicionarse en medio de la conexión, los datos estarán cifrados a conciencia. Como la mayoría de los hackers persiguen objetivos fáciles, probablemente se desharán de la información robada en lugar de comenzar un largo proceso de descifrado.
- **Uso de conexiones SSL:** No es habitual disponer de una conexión VPN para navegar por Internet, pero podemos agregar una capa de cifrado a la comunicación. Tenemos que activar la opción "**Usar siempre HTTPS**" en los sitios web que visitemos con frecuencia, o en los que haya que introducir contraseñas. La mayoría de los sitios web que requieren una cuenta o contraseñas cuentan con la opción "HTTPS" en alguna parte de su configuración.
- **Desactivación del uso compartido:** Cuando nos conectamos a Internet en un lugar público, es poco probable que queramos compartir algo. Podemos desactivar el uso compartido de datos en las preferencias del sistema o en el Panel de Control, en función del sistema operativo, o bien dejar que Windows lo desactive mediante la selección de la opción de "**pública**" la primera vez que nos conectemos a una nueva red no segura.
- **Mantenimiento de la opción Wi-Fi desactivada cuando no la necesitamos:** Aunque no estemos utilizando la conexión inalámbrica, nuestro equipo continúa transmitiendo datos con cualquier red dentro de su rango de alcance. Por lo tanto, si no necesitamos la conexión, mejor desactivar el Wi-Fi. Además de estar más seguros, la batería durará más.
- **Protección ante todo:** Si vamos a utilizar mucho las redes Wi-Fi públicas, es aconsejable instalar en nuestro equipo una solución de seguridad en Internet sólida.

3.3.5. Técnicas de seguridad biométrica

Los sistemas de autenticación se dividen en tres grupos:

- Uso de contraseña
- Uso de tarjetas
- Reconocimiento físico del usuario

Los sistemas biométricos pertenecen al último grupo. Se basan en el reconocimiento de características del usuario como su firma, su huella dactilar, su iris, Las técnicas de identificación biométrica tienen la ventaja de que los patrones no pueden perderse o ser sustraídos, ni pueden ser usados por otros individuos en el caso de que lleguen a tener acceso a ella. Por lo tanto, el problema de suplantación de identidad queda resuelto. Además, son los más cómodos de utilizar para los usuarios, ya que eliminan la necesidad de recordar contraseñas o números de identificación y la posibilidad de olvido en casa de la tarjeta. Aunque este sistema es el más seguro, tiene el inconveniente de su elevado coste, su dificultad de mantenimiento y la posibilidad de que el sistema rechace a un usuario válido.

4. USO SEGURO DE LA WEB

4.1. CONVENIENCIA DE HACER ACTIVIDADES EN LÍNEA EN SITIOS WEB SEGUROS



Hay que tener mucho cuidado a la hora de dar información personal en una página web. Comprobad que sea un sitio web protegido y no deis ninguna información que no sea estrictamente necesaria.

Los sitios web con protección utilizan el protocolo HTTPS en lugar del HTTP, indicando que la transferencia de datos es segura. Lo podéis ver en la dirección. Lo utilizan, por ejemplo, las entidades bancarias.

Las páginas web son seguras si tienen certificado de seguridad. Veréis un icono (🔒) a la derecha de la barra de direcciones. Clicando este icono os dará información. Las páginas seguras siguen el protocolo SSL (Secure Socket Layers) de encriptación que cifra la información, protegiéndola y evitando que pueda ser interceptada. Esto es importante cuando tenemos que introducir datos privados como el número de la tarjeta de crédito. Las conexiones SSL las distinguiréis porque la dirección comienza con "https://" en lugar de "http://".

Si la página tiene certificado de seguridad, toda la información que introducís, tanto en el formulario de registro como en el de aceptación de pedido, irán protegidos con el protocolo SSL. Esto significa que la información que viaja a través de Internet, de vuestro ordenador hasta el servidor de la página, lo hace de forma codificada.

Este sistema requiere que el servidor esté acreditado mediante un certificado electrónico expedido por una autoridad de certificación, que garantiza que se está accediendo a un servidor seguro.

Un certificado digital es un archivo electrónico que identifica de forma exclusiva a individuos y páginas web en Internet y permite establecer comunicaciones confidenciales y seguras. Los certificados digitales funcionan como una forma de credencial o pasaporte digital.

Una autoridad de certificación (CA, Certification Authority) es una entidad que se encarga de autenticar los participantes de las transacciones que se hacen en Internet. La CA se encarga de emitir los certificados a los usuarios, para que estos los puedan utilizar en sus comunicaciones seguras con otros usuarios de la red.

Los certificados SSL autenticados permiten:

- Comunicarse de forma segura con el sitio web, de manera que la información suministrada por el usuario no pueda ser interceptada durante la transmisión (confidencialidad) ni alterada sin que nadie lo detecte (integridad).
- Comprobar que el sitio que el usuario está visitando realmente pertenece a la empresa y que no ha sido suplantada (autenticación).

El protocolo SSL se basa en un sistema dual de clave pública y privada para garantizar una compra segura. La información en su tránsito por Internet, no es más que un conjunto de datos sin sentido e indescifrable. Aunque en el caso que pudieran ser copiados, nunca se podrían interpretar: la información permanece segura y privada.

4.2. PHARMING

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS o de los equipos de los usuarios. El atacante redirige el nombre de dominio a otra máquina. De esta forma, un usuario que introduzca un determinado nombre de dominio (que ha sido redirigido), accederá a la página web que el atacante haya especificado para ese nombre de dominio.

Los ordenadores conectados a Internet tienen una dirección IP única, que consiste en 4 grupos de 8 dígitos binarios de 0 a 255 separados por un punto (por ejemplo: 156.1.0.5). Estas direcciones IP son comparables a las direcciones postales de las casas, o al número de los teléfonos.

Debido a la dificultad que suponía para los usuarios tener que recordar esas direcciones IP, surgieron los Nombres de Dominio, que van asociados a las direcciones IP, del mismo modo que los nombres de las personas van asociados a sus números de teléfono en una guía telefónica.

Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados, o bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix.

La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

Algunos de los métodos tradicionales para combatir el pharming son:

- Utilización de software especializado (**protección DNS**): suele utilizarse en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing.
- Uso de **addons** para los navegadores web como, por ejemplo, toolbars: permite a los usuarios domésticos protegerse de esta técnica. Para IExplorer podéis ver algunas soluciones aquí: <http://www.iegallery.com/es-es/trackingprotectionlists>

Tened presente que los filtros anti-spam normalmente no protegen contra esta técnica.

A nivel de usuario, podéis usar el comando **tracroute** (para UNIX, MAC y GNU/Linux) o **tracert** (para Windows) que permite observar mediante direcciones IP hacia donde se dirigen nuestras peticiones y, de este modo, comprobar la integridad del servidor al que se dirige nuestro acceso.

- **En Windows:** ejecutad la consola de comandos (cmd) y ejecutad el comando. Por ejemplo, para la dirección de Google, escribiremos: C:\>tracert www.google.com
- **En GNU/Linux:** user@localhost:/# traceroute www.google.com
- **En Mac:** En **Aplicaciones**, escoged **Utilidades** y abrid la aplicación **Utilidad de Red**. En la pestaña **Traceroute**, escribid el dominio o IP y se empezará a trazar la ruta.

4.3. CERTIFICADO DIGITAL

Algunos trámites hechos por Internet implican una transacción de datos que conviene proteger y autenticar. Los certificados digitales aseguran la integridad del contenido y la autenticación del remitente y el receptor.

La firma digital es un mecanismo de cifrado para autenticar información digital. Adjuntando la firma digital a los mensajes conseguimos que el receptor esté seguro de que el mensaje proviene de la persona indicada en el remite y que el mensaje no ha sido alterado durante la transmisión.

Podéis obtener el certificado digital e información en el Portal de Administración electrónica (Gobierno de España):

<http://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>

4.4. CONTRASEÑA DE UN SOLO USO

Este tipo de contraseña (OTP: One-Time Password) es válida sólo una vez. Respecto a la tradicional contraseña, la principal ventaja es que no será vulnerable a ataques de REPLAY ya que, al cambiarla, los intentos anteriores para descubrir la contraseña anterior son inútiles y hay que empezar de nuevo. El inconveniente es que no podemos memorizar todas las contraseñas posibles y, por lo tanto, necesitaremos una tecnología adicional para averiguarla.

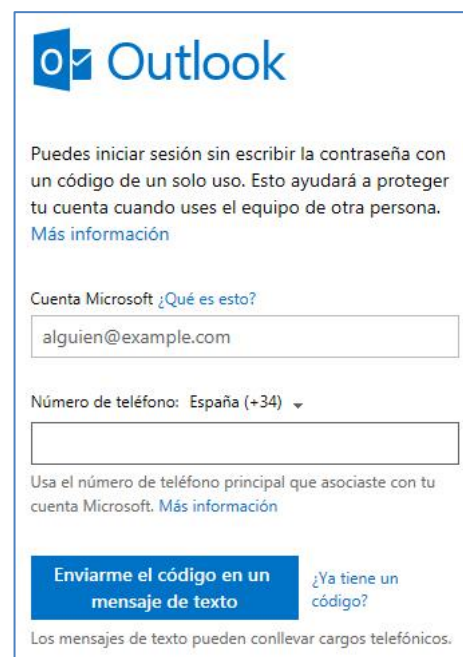
Para las cuentas de correo **Hotmail** o **Outlook** podéis usar contraseñas de un solo uso con vuestro móvil:

En la pantalla de inicio de sesión, escribid vuestro correo y clicad el enlace **Inicia sesión con un código de un solo uso**:



The screenshot shows the Outlook login interface. At the top is the Outlook logo. Below it, the text 'Cuenta Microsoft ¿Qué es esto?' is followed by a text input field containing 'Correo electrónico o teléfono'. Below this is another text input field for 'Contraseña'. A checkbox labeled 'Mantener la sesión iniciada' is present. A blue button labeled 'Iniciar sesión' is at the bottom. Below the button, there is a link '¿No puedes acceder a tu cuenta?' and a link 'Inicia sesión con un código de un solo uso'.

En la siguiente pantalla, introducíd vuestro número de teléfono (sólo funciona para móviles) y clicad el botón **Enviarme el código en un mensaje de texto**.




The screenshot shows the next step in the Outlook login process. It features the Outlook logo and the text 'Puedes iniciar sesión sin escribir la contraseña con un código de un solo uso. Esto ayudará a proteger tu cuenta cuando uses el equipo de otra persona. Más información'. Below this is a text input field for 'Cuenta Microsoft ¿Qué es esto?' containing 'alguien@example.com'. A dropdown menu for 'Número de teléfono: España (+34)' is shown. Below the dropdown is a text input field for the phone number. A note states 'Usa el número de teléfono principal que asociaste con tu cuenta Microsoft. Más información'. At the bottom, there is a blue button labeled 'Enviarme el código en un mensaje de texto' and a link '¿Ya tiene un código?'. A footer note says 'Los mensajes de texto pueden conllevar cargos telefónicos.'

Recibiréis, en vuestro teléfono, un mensaje con la contraseña. Esta opción es útil cuando tenemos que conectarnos desde un equipo del que no sabemos si es seguro. El número de teléfono ha de ser el que disteis al crear la cuenta.

4.5. AUTOCOMPLETADO EN UN FORMULARIO

En muchas páginas web tenemos que rellenar formularios y se nos hace muy pesado. La función **Autocompletar** puede ayudarnos rellenando los formularios automáticamente, a partir de lo que empezamos a escribir ya que recuerda lo que hemos escrito anteriormente.

Para **activar/desactivar Autocompletar en Ms Edge** seguid estos pasos:

- Clicad el botón **Más Acciones** .
- Escoged la opción **Configuración**.
- Clicad el botón **Ver configuración avanzada**.
- Buscad la opción **Guardar las entradas de formularios** y la activáis o desactiváis según convenga.

Guardar las entradas de formularios



Activado

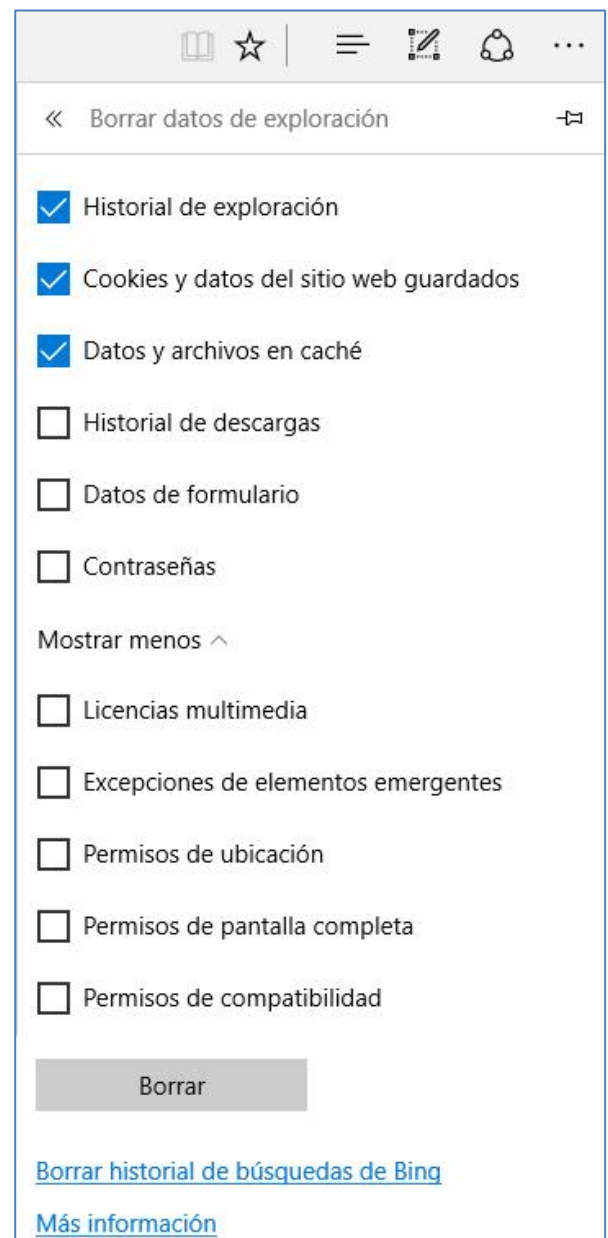
Utilizad el botón **Elegir lo que se debe borrar** cuando queráis limpiar la lista que tenéis en ese momento. Lo encontraréis en la opción **Configuración** del botón **Más Acciones**.

En la ventana que aparece, activad las opciones que queráis limpiar (para el autocompletado de formularios, la opción es **Datos de formulario**).

Antes de presionar el botón **Borrar**, comprobad si queréis eliminar el resto de opciones que están marcadas; si no es así, desactivadlas antes de presionar el botón.

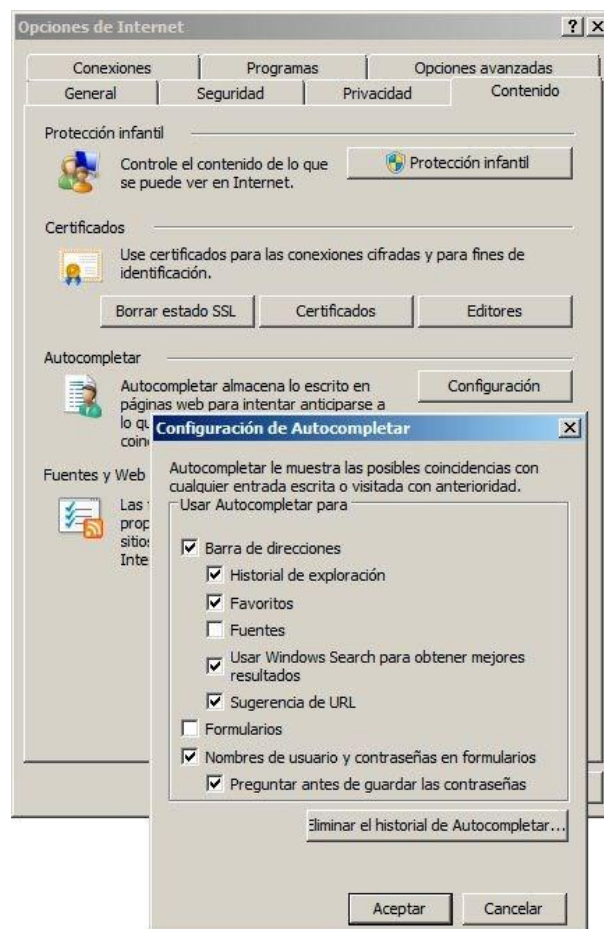
Fijaos que en este cuadro de diálogo podéis eliminar también las contraseñas guardadas y las cookies.

Con **Internet Explorer** encontraréis estas opciones en **Opciones de Internet** del menú **Herramientas**. En el cuadro de diálogo que aparece, activad la pestaña **Contenido** y, en el apartado **Autocompletar**, clicad el botón **Configuración**.



Para **activar/desactivar Autocompletar en Internet Explorer** seguid estos pasos:

- Abrid Internet Explorer.
- Escoged **Opciones de Internet** en el botón **Herramientas** (⚙️).
- En la pestaña **Contenido**, en **Autocompletar**, clicad el botón **Configuración**. Activad o desactivad la opción **Formularios**.

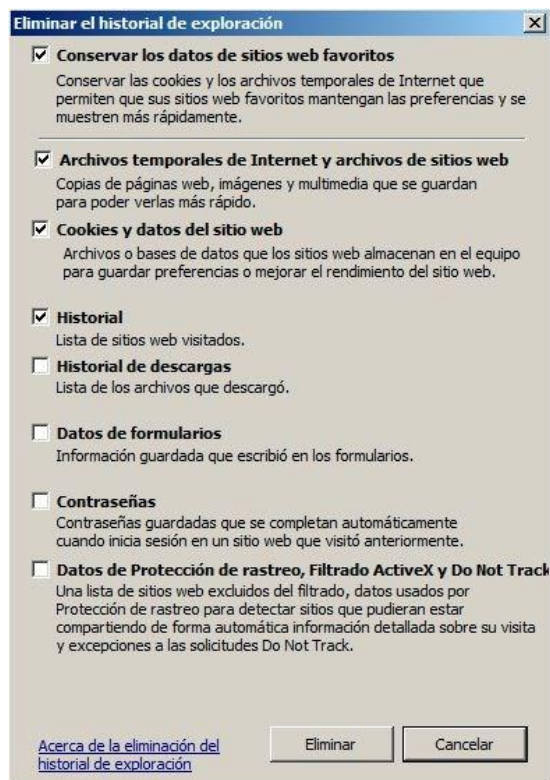


Utilizad el botón **Eliminar el historial de Autocompletar** cuando queráis limpiar la lista que tenéis en aquel momento.

En el cuadro de diálogo que aparece, activad las opciones que queráis limpiar (para el autocompletado de formularios, la opción es **Datos de formularios**).

Antes de presionar el botón **Eliminar**, comprobad si queréis eliminar el resto de opciones que están marcadas; si no es así, desactivadlas antes de presionar el botón.

Fijaos que en este cuadro de diálogo podéis eliminar también las contraseñas guardadas y las cookies.



4.6. COOKIES

Una galleta (*cookie*) es un archivo que envían los servidores de Internet en el que se almacena (en el navegador del usuario) información sobre la actividad del usuario (explorador utilizado, webs más visitadas, ...).

El navegador web permite aceptar, bloquear y eliminar las cookies. Normalmente, al entrar en un sitio web que usa cookies, el navegador nos preguntará si las aceptamos o no. Si hemos aceptado, por error, las cookies de un sitio web podemos eliminarlas.

Las cookies las podemos clasificar de diferentes maneras:

- **Según la entidad que las gestiona:**
 - Propias: Las que se envían al equipo del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario.
 - De terceros: Las que se envían al equipo del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos a través de las cookies.
- **Según el tiempo que permanecen activadas:**
 - De sesión: Las que están diseñadas para recoger datos mientras el usuario accede a una página web. Almacenan información que sólo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión como, por ejemplo, la lista de productos adquiridos.
 - Persistentes: Las que están diseñadas para que los datos sigan almacenados en el equipo y puedan ser tratados durante un periodo definido por el responsable de la cookie.
- **Según su finalidad:**
 - Técnicas: Las que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan como, por ejemplo, recordar los elementos que integran un pedido o realizar el proceso de compra de un pedido.
 - De personalización: Las que permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el equipo del usuario como, por ejemplo, el idioma o el tipo de navegador a través del cual accede al servicio.
 - De análisis: Las que permiten al responsable, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.

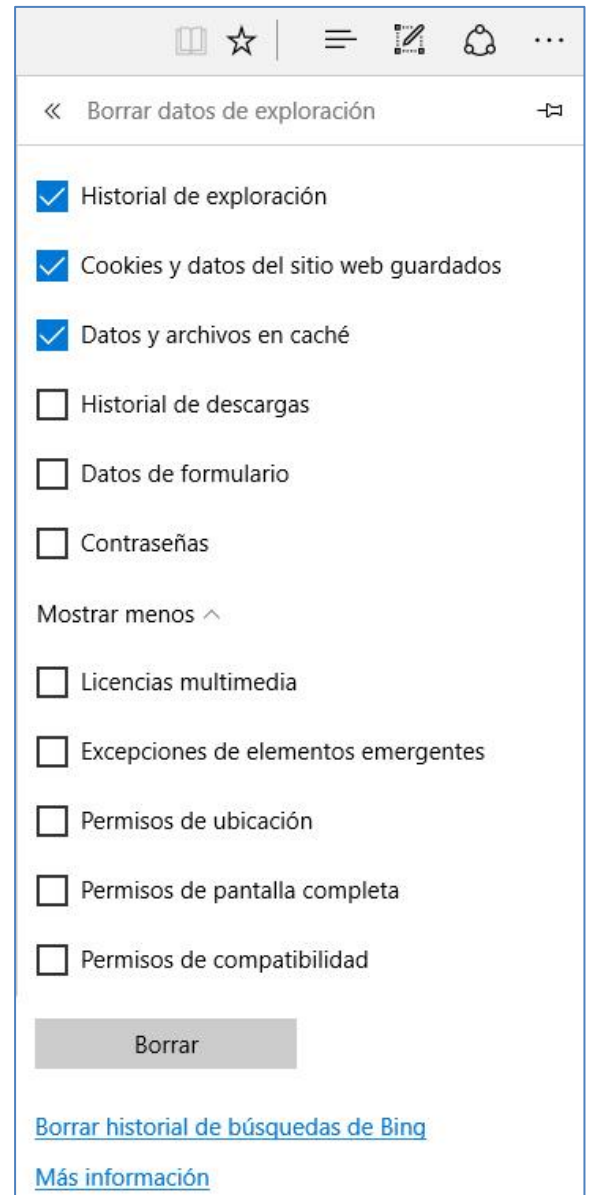
En **Ms Edge** podéis bloquear y eliminar las cookies de la siguiente manera:

Eliminar las cookies:


Utilizad el botón **Elegir lo que se debe borrar** que encontraréis en la opción **Configuración** del botón **Más Acciones**.

En la ventana que aparece, activad sólo la opción **Cookies y datos del sitio web guardados**.

El inconveniente es que eliminaremos todas las cookies, no podemos escoger las que queremos eliminar.



Bloquear cookies:


- Clicad el botón **Más Acciones** .
- Escoged la opción **Configuración**.
- Clicad el botón **Ver configuración avanzada**.
- Buscad la opción **Cookies** e indicad si las queréis bloquear todas o sólo las de terceros.



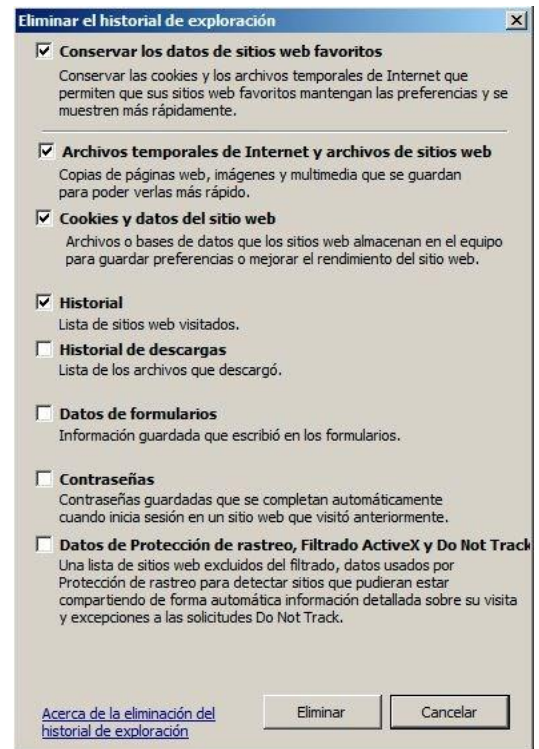
Al bloquear las cookies, es posible que algunas páginas no se muestren correctamente o que aparezca un mensaje que informe de que es necesario permitir las cookies para poder ver el sitio.

En **Internet Explorer** podemos aceptar, bloquear y eliminar las cookies de la siguiente manera:


Eliminar las cookies:

- Escoged **Opciones de Internet** en el botón **Herramientas** ()
- En la pestaña **General**, en **Historial de exploración**, clicad el botón **Eliminar....** Activad la opción **Cookies y datos del sitio web**. Desactivad el resto de opciones antes de presionar el botón **Eliminar**.


El inconveniente es que eliminaremos todas las cookies, no podemos escoger las que queremos eliminar.

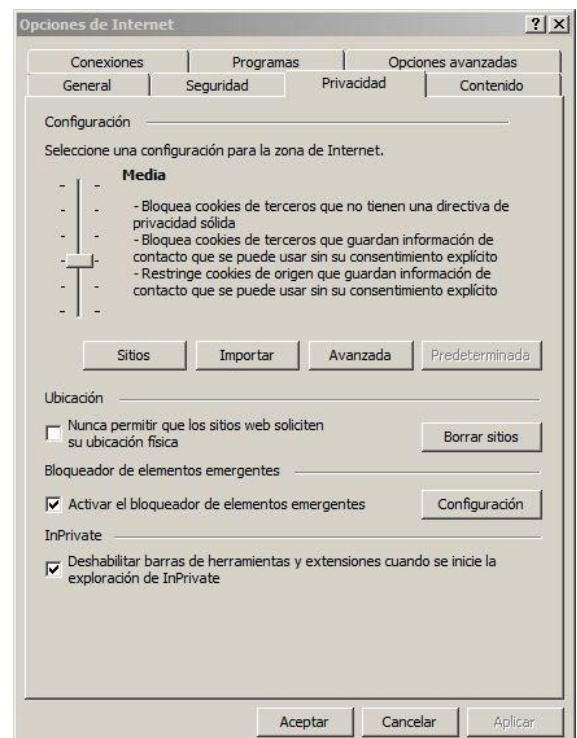


Bloquear cookies:

- Escoged **Opciones de Internet** en el botón **Herramientas** ()
- En la pestaña **Privacidad**, en **Configuración**, moved el control de nivel para escoger el tipo de cookies que queréis bloquear. Si lo movéis totalmente hacia arriba, las bloquearéis todas.

Permitir cookies:

- Escoged **Opciones de Internet** en el botón **Herramientas** ()
- En la pestaña **Privacidad**, en **Configuración**, moved el control de nivel totalmente hacia abajo para permitir todas las cookies.

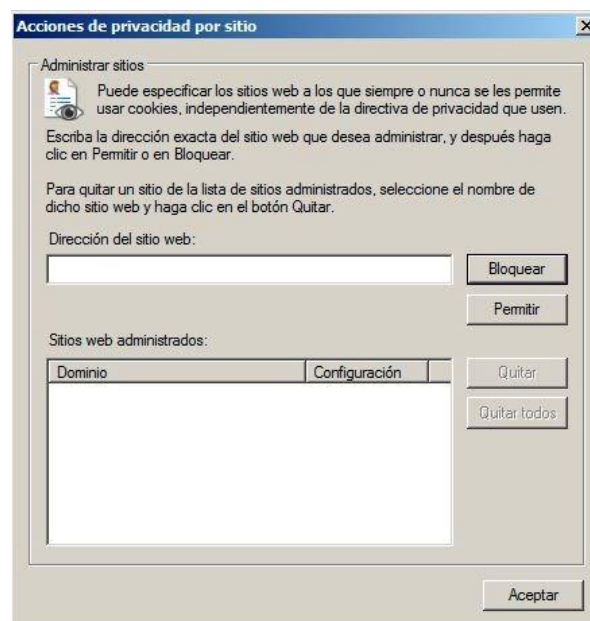


Al bloquear las cookies, es posible que algunas páginas no se muestren correctamente o que aparezca un mensaje que informe que es necesario permitir las cookies para poder ver el sitio.

En la pestaña **Privacidad**, clicando el botón **Sitios**, podéis permitir o bloquear cookies para sitios web específicos.

Escribid la dirección del sitio web y clicad el botón correspondiente.

En la parte inferior veréis las configuraciones escogidas.



Podéis ver un **informe de privacidad** de una página web para ver los sitios que tienen contenido en la página y las cookies almacenadas en el equipo después de visitar la página:

- Escoged **Seguridad** en el botón **Herramientas** (⚙️).
- Escoged la opción **Directiva de privacidad de páginas web**.



4.7. SOFTWARE PARA CONTROLAR CONTENIDOS DE INTERNET

La mayor preocupación de los padres respecto al uso del ordenador y de Internet por parte de sus hijos es cómo pueden controlar el tiempo de uso y el contenido al que acceden.

Windows 10 permite establecer límites al uso del ordenador y aumentar la seguridad mientras están conectados, sin necesidad de vigilarlos constantemente. Permite limitar el tiempo que pasan delante del ordenador, controlar los programas y juegos que pueden utilizar y cuándo,...

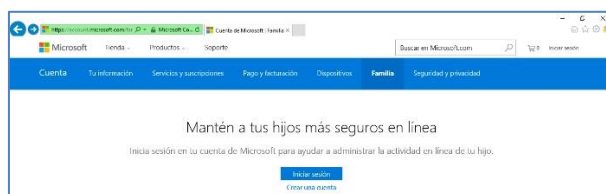
Si habéis trabajado con versiones anteriores de Windows, tened presente que el control parental ahora se hace de una manera muy diferente, ya no existe el Panel de control **Control parental**.

Para usar el control parental en Windows 10, es necesario que vosotros y vuestros hijos tengáis una cuenta Microsoft. Podéis crearlas aquí: <https://www.microsoft.com/es-es/outlook-com/>

4.7.1. Configurar el Control parental

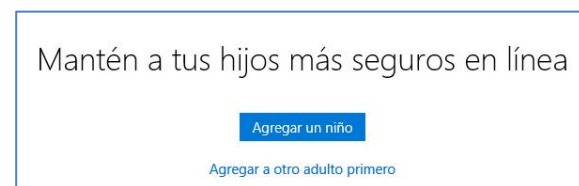
La primera vez que configuréis el control parental, conectaos a la página web de Microsoft que lo gestiona:

<https://account.microsoft.com/family/about>



Clicad en **Iniciar sesión** y escribid vuestro correo Outlook y vuestra contraseña. Si todavía no lo tenéis, lo podéis crear en esta misma página.

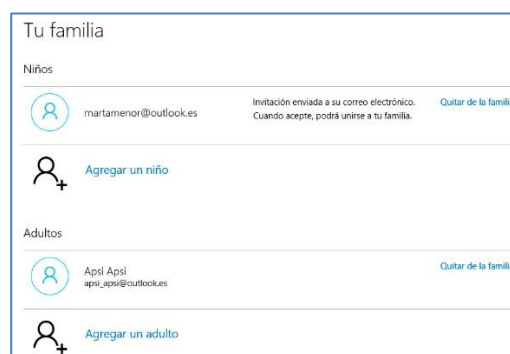
Primero os preguntará si queréis añadir a un menor o a un adulto.



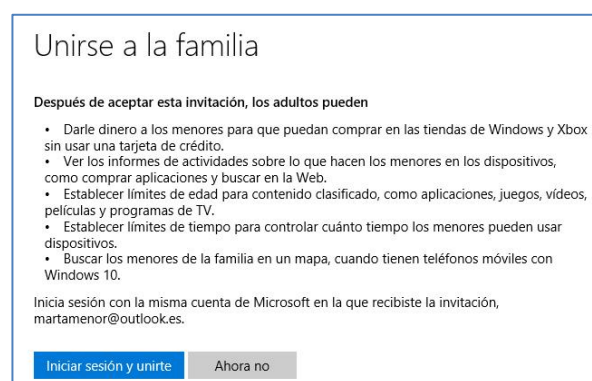
Pedirá que escribáis la dirección de correo del usuario que queréis añadir (correo Outlook).

A screenshot of a form titled 'Agregar un niño'. The form has a blue border and a white background. At the top, it says 'Agregar un niño'. Below this, it says 'Cuando tu hijo acepta la invitación, los adultos de la familia pueden' followed by a bulleted list of permissions: 'Darle dinero a los menores para que puedan comprar en las tiendas de Windows y Xbox sin usar una tarjeta de crédito.', 'Ver los informes de actividades sobre lo que hacen en los dispositivos, como comprar aplicaciones y buscar en la Web.', 'Establecer límites de edad para contenido clasificado, como aplicaciones, juegos, videos, películas y programas de TV.', 'Establecer límites de tiempo para controlar cuánto tiempo pueden usar dispositivos.', and 'Encontrarlos en un mapa, si tienen teléfonos móviles con Windows 10.' Below the list, it says 'Si tu hijo tiene una dirección de correo electrónico, úsala para invitarlo a la familia.' and there is a text input field containing 'martamenor@outlook.es' with a small 'x' icon to its right. Below the input field, it says 'Crea una nueva dirección de correo electrónico para tu hijo'. At the bottom, there are two buttons: 'Enviar invitación' and 'Cancelar'.

Ya tenéis activado el control parental para esta cuenta. Si queréis añadir más cuentas al control parental, utilizad los enlaces **Agregar un niño** y **Agregar un adulto**.

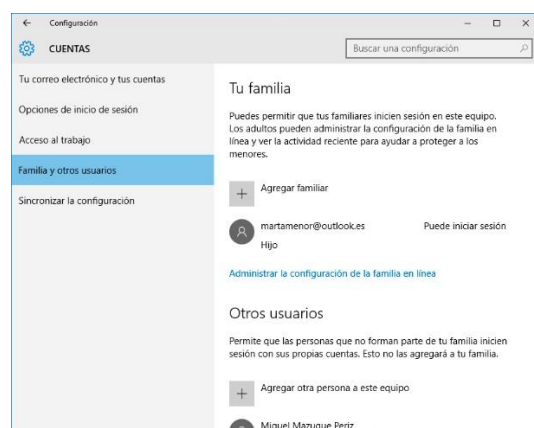


El usuario de la cuenta recibirá un mail con la invitación. Una vez aceptada, ya tendréis acceso al control parental de esta cuenta:

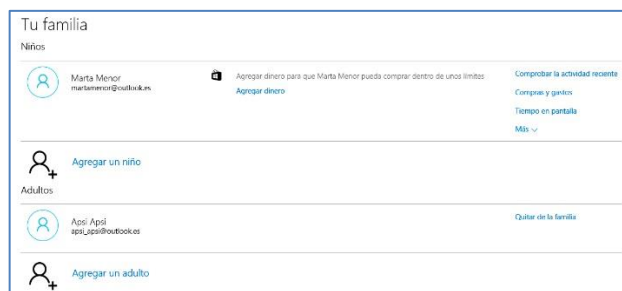


4.7.2. Administrar las cuentas añadidas al Control parental

Para administrar y añadir más cuentas al Control parental, lo podéis hacer conectándoos a la página web de Microsoft (<https://account.microsoft.com/family/about>) o desde la configuración de vuestro Windows: **Inicio - Configuración - Cuentas:**



En la categoría **Familia y otros usuarios** (apartado **Tu familia**) clicad el enlace **Administrar la configuración de la familia en línea**.

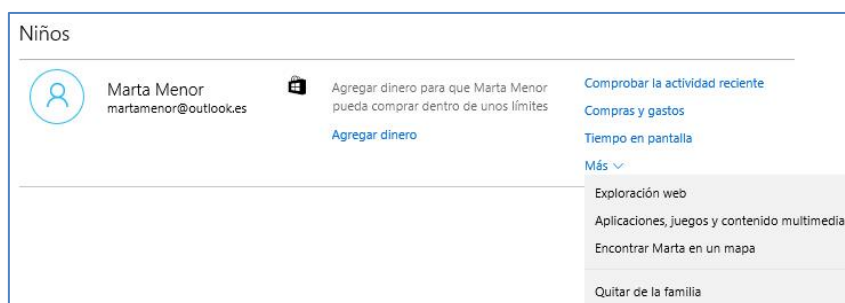


Podéis añadir más cuentas al control parental con los enlaces **Agregar un niño** y **Agregar un adulto**, quitar cuentas de este control parental (**Quitar de la familia**) y, si es un menor, gestionar la cuenta.

Fijaos que sólo podéis gestionar las cuentas de los menores. Las cuentas de adultos sólo las podéis quitar de la familia.

4.7.3. Gestionar la cuenta de un menor

Al acceder al administrador de las cuentas de la familia encontraréis, para las cuentas de los menores, enlaces que os permiten gestionarlas:



Agregar dinero: Permite transferir dinero a la cuenta para hacer pagos en la tienda de Microsoft.

Comprobar la actividad reciente: Si habilitáis esta función, os mostrará un informe de la actividad (en el ordenador y en el móvil, si tiene Windows 10) de esta cuenta (sitios web visitados, aplicaciones y juegos utilizados y tiempo en pantalla):



Podéis pedir la recepción de informes por correo electrónico y activar el bloqueo de páginas web y aplicaciones y la limitación de horas.

Compras y gastos: Muestra el historial de compras de la cuenta y permite transferir dinero.

Tiempo en pantalla: Permite activar la limitación de horas de uso del dispositivo e indicar a qué horas permitís el acceso al ordenador para este usuario. Si la sesión está iniciada cuando finalice el tiempo asignado, se cerrará automáticamente:

Establecer límites para cuando mi hijo puede usar dispositivos

☒ Habilitado

Se aplica a:

PC Windows 10

Elige las horas en las que Marta Menor puede usar dispositivos

	Como muy pronto a las	No más tarde de	Limitar por día en este dispositivo
Domingo	7:00 a.m.	10:00 p.m.	Sin límites
Lunes	7:00 a.m.	10:00 p.m.	Sin límites
Martes	7:00 a.m.	10:00 p.m.	Sin límites
Miércoles	7:00 a.m.	10:00 p.m.	Sin límites
Jueves	7:00 a.m.	10:00 p.m.	Sin límites
Viernes	7:00 a.m.	10:00 p.m.	Sin límites
Sábado	7:00 a.m.	10:00 p.m.	Sin límites

Más – Exploración web: Permite activar el bloqueo de páginas web e indicar qué direcciones web puede visitar y cuáles no. Sólo funciona para Internet Explorer y Microsoft Edge:

Bloquear sitios web inapropiados

☒ Activado

Se aplica a:

PC y móvil con Windows 10

El contenido para adultos está **bloqueado**

Búsqueda segura está activado

Los sitios web solo se pueden bloquear en Internet Explorer o en Microsoft Edge. Para proteger a tu hijo, bloquea cualquier otro explorador que aparezca en la opción **Actividades recientes** que encontrarás en **Aplicaciones y juegos**.

Permitir siempre estos

Escribe la dirección URL de un sitio web que quieres permitir:

example.com

No hay sitios web en la lista de permitidos.

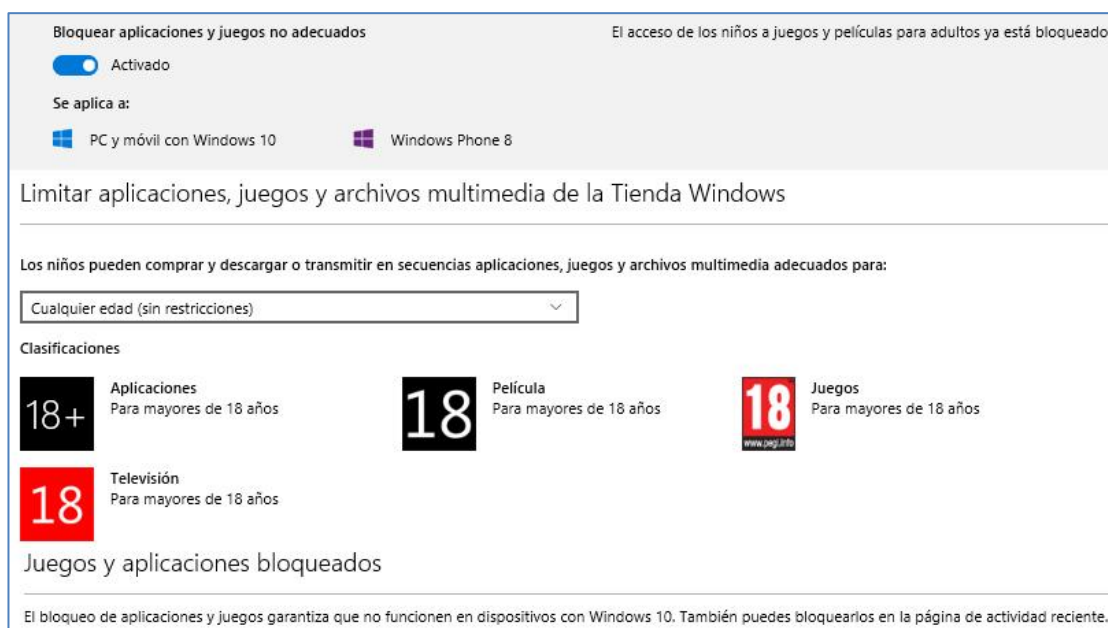
Bloquear siempre estos

Escribe la dirección URL de un sitio web que quieres bloquear:

example.com

No hay sitios web en la lista de bloqueados.

Más – Aplicaciones, juegos y contenido multimedia: Permite activar el bloqueo automático de aplicaciones, juegos y archivos multimedia e indicar la edad del menor:



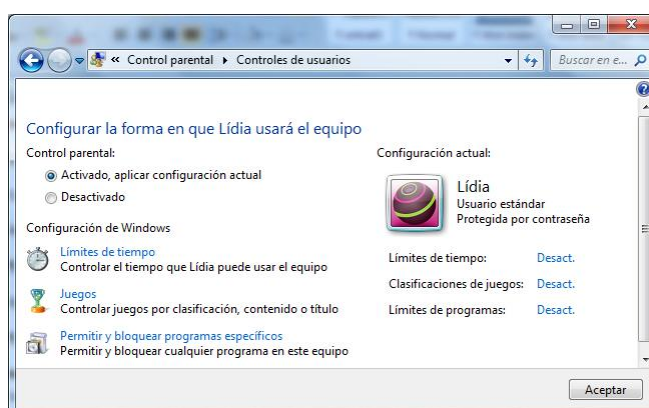
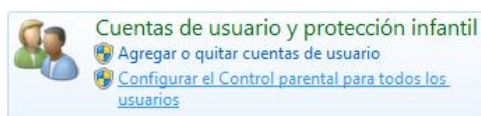
Más – Encontrar “nom del menor” en un mapa: Permite activar el localizador del móvil del menor. Sólo se puede hacer si el móvil del menor tiene Windows 10 Mobile y ha iniciado la sesión del móvil con una cuenta Microsoft.

Más – Quitar de la familia: Permite eliminar la cuenta del control parental.

4.7.4. El control parental en Windows 7

Como activar el Control parental para una cuenta de usuario en Windows 7:

1. Abrid el **Panel de control (Iniciar)**.
2. En el apartado **Cuentas de usuario y protección infantil**, clicad en **Configurar el Control parental para todos los usuarios**.
3. Escoged la cuenta de usuario que queréis controlar.
4. Activad la opción **Activado, aplicar configuración actual**.



5. Ajustad los 3 apartados de la configuración según vuestras necesidades:

Límites de tiempo: Clicad en las casillas de la cuadrícula para indicar a qué horas permitís el acceso al ordenador para este usuario.

Si la sesión está iniciada cuando finalice el tiempo asignado, se cerrará automáticamente.

Controlar el tiempo que Lidia podrá usar el equipo

Haga clic y arrastre las horas que desee bloquear o permitir.

	Hora	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
lunes																										
martes																										
miércoles																										
jueves																										
viernes																										
sábado																										
domingo																										

☐ Permitido
☒ Bloqueado

Juegos: Podéis indicar que el usuario no pueda jugar a ningún juego (**No**) o seleccionar los juegos a los que puede acceder (**Sí**).

Con la opción **Establecer clasificación de juego**, podéis indicar los juegos aceptados a partir de su clasificación por edades y contenido.

Con la opción **Bloquear o permitir juegos específicos**, podéis indicar a qué juegos, de los instalados en el ordenador, puede jugar.

Controlar el tipo de juegos a los que Lidia puede jugar

¿Lidia puede jugar a cualquier juego?

☒ Sí
☐ No

Bloquear (o permitir) juegos por clasificación y tipos de contenido

[Establecer clasificación de juego](#)

Clasificación máxima permitida: 18+, incluidos los juegos sin clasificar
Descriptor de juegos bloqueados: Ninguno

Bloquear (o permitir) cualquier juego en el equipo por nombre

[Bloquear o permitir juegos específicos](#)

Siempre bloqueado: Ninguno
Siempre permitido: Ninguno

Permitir o bloquear programas específicos:

Podéis indicar qué programas, de los instalados en el ordenador, puede utilizar el usuario.

¿Qué programas puede usar Lidia?

☐ Lidia puede usar todos los programas.
☒ Lidia solo puede usar los programas permitidos

Comprobar los programas que se pueden usar

Archivo	Descripción
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE11\...	
<input checked="" type="checkbox"/> ACECNFLT.EXE	Replication Conflict Viewing and
<input checked="" type="checkbox"/> MSE7.EXE	Microsoft Script Editor
<input checked="" type="checkbox"/> MSOICONS.EXE	2007 Microsoft Office componen
<input checked="" type="checkbox"/> MSOXMLED.EXE	XML Editor
<input checked="" type="checkbox"/> ODSERV.EXE	Microsoft Office Diagnostics
<input checked="" type="checkbox"/> OFFDIAG.EXE	Microsoft Office Diagnostics
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE11\...	
<input checked="" type="checkbox"/> ODEPLOY.EXE	Microsoft Office Multi-Msi Active
<input checked="" type="checkbox"/> SETUP.EXE	Microsoft Setup Bootstrapper
C:\Program Files (x86)\Common Files\microsoft shared\Smart Ta	
<input checked="" type="checkbox"/> SmartTagInstall.exe	Microsoft Office 2010 componen

Agregar un programa a la lista:

4.8. REDES SOCIALES

En Internet, las comunidades virtuales, comunidades en línea o redes sociales son grupos de personas con las que se comparte algún interés y que se ponen en contacto a través de sitios web, fórums, blogs, chats, juegos en línea...

Los **objetivos** principales de la comunidad virtual son los siguientes:

- Intercambiar información.
- Ofrecer apoyo.
- Conversar y socializar de manera informal.
- Debatir.

Ejemplos: Facebook, Twitter, Wikipedia, Windows Live Messenger,...

Precauciones:

Para adherirse a una comunidad hay que registrarse y, por lo tanto, dar una serie de datos personales. Hay que ir con mucho cuidado con la información que damos y no dar más de la que sea estrictamente necesaria. No hay que olvidar que no sabemos quién accederá a esta información. También hay que ser muy prudente a la hora de admitir nuevos contactos en las redes como Facebook si no queremos que desconocidos accedan a nuestra información personal.

Antes de crear o usar una cuenta en una red social, tened presentes los siguientes consejos:

- **Mantened actualizado vuestro sistema operativo, navegador y antivirus:** Las sucesivas actualizaciones del sistema operativo o del navegador añaden nuevas protecciones que nos serán muy útiles para nuestra seguridad.
- **Cuidad vuestra privacidad:** Pensad bien que datos personales ponéis en vuestro perfil de la red social; no olvidéis que pueden verlos cualquiera.
- **Evitad contactar con extraños:** Al recibir invitaciones de personas desconocidas, no os importe rechazarlas hasta que sepáis quién las envía realmente.
- **No suplantéis la identidad ajena:** Si suplantáis la identidad de alguien (famoso o desconocido) podríais tener problemas por derechos de autor y suplantación de identidad, con serios problemas legales.
- **No ofendáis ni compartáis contenidos inapropiados:** Respetad a los demás y no reveléis datos privados de los demás.
- **Pensadlo bien antes de subir una foto:** Normalmente, todo el material subido pasa a ser propiedad de la empresa que gestiona la red social. Pueden usar vuestras fotos para publicidad o cualquier otro propósito sin que se pueda evitar. Además, las fotos incluyen mucha más información de la que nos imaginamos (puede verse nuestra dirección, la matrícula de nuestro coche,...).

En realidad, las precauciones que debemos seguir son las mismas que seguimos en nuestra vida diaria.

Potenciales peligros:

A continuación os ponemos una lista de los peligros que nos podemos encontrar en las redes sociales:

- **Cyberbullying** (acoso en línea): A diario se envían mensajes intimidatorios y humillantes a través de las redes sociales, sobre todo a adolescentes. Secretos descubiertos, rumores falsos, reputaciones arruinadas, hostigamiento son cada vez más habituales. Cuando se trata de acoso a menores, se denomina **Grooming**.
- **Incitación al odio**: Los mensajes de odio, intolerancia y llamadas a la violencia contra una persona o grupos a causa de su raza, religión, nacionalidad o ideas políticas, se multiplican y amplifican en las redes sociales aprovechando el anonimato, la rapidez y el alcance mundial.
- **Rechazos laborales**: Las oficinas de recursos humanos están cada vez más atentas a las redes sociales y a lo que allí hacen o dicen sus futuros empleados. Los perfiles pueden ayudar a los reclutadores a conocer mejor a sus aspirantes y restarles puntos.
- **Phishing**: El usuario es llevado al engaño haciéndole revelar todos los datos de acceso de su cuenta mediante la invitación a una página falsa idéntica a la de su red social. El usuario creerá que se trata de un sitio de confianza e iniciará sesión normalmente. Normalmente, una vez que los datos son obtenidos, la página redirecciona al sitio original y el usuario no se habrá dado cuenta.
- **Malware**: El típico es el comentario que aparece en nuestra red social invitando a ver un video mediante un enlace a una web que a su vez pide instalar un códec para ver correctamente el sitio. Con falsas promesas como la de enterarse quién visitó nuestro perfil, ver las respuestas a preguntas que nuestros amigos han contestado sobre nosotros, imágenes divertidas o noticias sorprendentes, somos atraídos a caer en estas trampas que terminan con nuestras cuentas infectadas.
- **Problemas de privacidad**: Mucha gente introduce demasiada información sobre sus vidas. Desde datos básicos y de contacto, hasta información acerca de sus amigos, sus trabajos, aficiones, rutinas y actividades contadas en fotos y comentarios. No debemos olvidar que no podemos saber cómo son administrados estos datos sensibles.
- **Pérdida de productividad**: Algunas personas no pueden controlar el tiempo que pasan revisando sus redes sociales, llegando incluso a interferir con otras actividades como el estudio y el trabajo. Por este motivo, cada vez hay más empresas que prohíben y bloquean el uso de las redes sociales por considerar que distraen y bajan la productividad de sus empleados.

5. COMUNICACIONES

5.1. CORREO ELECTRÓNICO

5.1.1. Cifrado/descifrado de un correo electrónico

Cifrar los correos es alterar el contenido de lo que escribimos y adjuntamos de tal forma que si alguien lo intercepta sea totalmente irreconocible e ilegible para él. El cifrado de nuestros mensajes de correo nos asegurará que sólo la persona a la que va destinado el correo pueda leerlo. Dado que los proveedores de correo no garantizan nuestra privacidad en los correos que tenemos almacenados en sus servidores, tendremos que ser nosotros mismos quienes nos la garanticemos.

Existen diversos tipos de cifrado, entre ellos el cifrado tradicional (cifrado simétrico) y el cifrado asimétrico. El cifrado asimétrico es de los más seguros existentes en la actualidad. El cifrado asimétrico consiste en lo siguiente:

- El remitente tendrá un par de claves únicas disponibles. Una de las claves será pública y la otra será privada.
- El destinatario también dispondrá de 2 claves únicas disponibles (igualmente, una pública y otra privada).
- Bajo ningún concepto ni el destinatario ni el remitente proporcionarán a terceros su clave privada. Es de vital importancia que sólo nosotros tengamos acceso a la clave privada.
- Tanto el destinatario como el remitente distribuirán públicamente su clave pública. Las pueden subir a un servidor de claves, enviarla vía mail, pasarla con un pendrive, ...
- El remitente redactará el mensaje al destinatario. Una vez escrito, lo cifrará con la clave pública del destinatario.
- El destinatario recibirá el correo cifrado del remitente. En principio no podrá leer el correo porque el contenido está cifrado. Para descifrar el mensaje, el destinatario usará su clave privada. La única forma de descifrar este mensaje será mediante la clave privada del destinatario.

Existen varias opciones para cifrar nuestro correo electrónico. Algunas de ellas son:

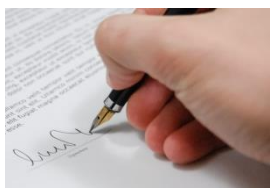
- **Para Microsoft Outlook:** podemos usar algunas extensiones como, por ejemplo, GP4Win y Outlook Privacy plugin. Outlook también permite cifrar y firmar mensajes de forma nativa.
- **Para Mozilla Thunderbird:** podemos usar la extensión Enigmail o WebPG for Mozilla. Enigmail es una buena opción ya que el proceso de cifrar es prácticamente automático y tiene la ventaja que el software usado es open source y multiplataforma. Las instrucciones para usar Enigmail las podéis ver en el web de Mozilla:

https://www.mozilla-hispano.org/documentacion/Firma_y_cifrado_de_correos_electr%C3%B3nicos#Firma_y_cifrado_con_GPG_y_Enigmail

Thunderbird también permite de forma nativa cifrar y firmar mails con S/MIME.

- **Para los navegadores Chrome, y Firefox:** Existen extensiones como, por ejemplo, Mailvelope o Secure Gmail.
- **Para Android:** podemos usar la aplicación de correo k9mail y el programa APG. El proceso de cifrar y firmar los mails es prácticamente automático y apenas genera molestias ni tener que realizar pasos adicionales.

5.1.2. Firma digital



La firma digital es un mecanismo de cifrado para autenticar información digital. Adjuntando la firma digital a los mensajes conseguimos que el receptor esté seguro de que el mensaje proviene de la persona que se indica en el remitente y que el mensaje no ha sido alterado durante la transmisión. Podéis consultar la información que da el *Portal*

Administración Electrónica (Gobierno de España):

<http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html>

5.1.3. Correos electrónicos fraudulentos y no solicitados

El correo basura (SPAM) son mensajes enviados indiscriminadamente y masivamente, sin el consentimiento de los receptores. Normalmente son mensajes comerciales, aunque también son frecuentes los engaños con intención de sacar provecho económico de las víctimas.

Es recomendable no contestar nunca al spam, ya que al remitente le puede servir de confirmación de que la dirección existe y está en uso. Tampoco cliquéis ningún enlace que contenga el mensaje ya que puede desencadenar una descarga peligrosa.

Las aplicaciones de correo pueden filtrar estos correos. Seleccionad el mensaje y buscad una opción que diga “Enviar a correo basura” o algo parecido; el mensaje lo guardará en una carpeta y, a partir de ahora, no os volverá a mostrar ningún mensaje de este remitente.

5.1.4. Phishing

El phishing es un fraude que se hace con un correo electrónico o mensajería instantánea con el que se piden datos sobre las tarjetas de crédito, claves bancarias, ... Los mensajes utilizan todo tipo de argumentos relacionados con la seguridad de la entidad para justificar la necesidad de introducir los datos de acceso. Por ejemplo, podéis recibir un correo con el logotipo del vuestro banco y que parezca realmente que os lo envía vuestro banco.

Recomendaciones:

- No respondáis a correos electrónicos escritos en otros idiomas: vuestro banco no os enviará un comunicado en otro idioma si no lo habéis pactado previamente.
- No respondáis a correos enviados por entidades de las que no sois cliente en los que os pidan datos.
- No atendáis de forma inmediata o impulsiva a correos que hablen de un sorteo o una oferta.
- No atendáis a correos que os avisen del cese de actividades financieras recibidos por sorpresa.
- No atendáis a correos que hagan sospechar sin confirmarlos por teléfono o personalmente.
- No entréis en la página web de vuestro banco a través de buscadores ya que podrían derivaros, sin daros cuenta, a una página falsa. Escribid la URL de vuestro banco en la barra de direcciones del explorador.
- Y, sobre todo, nunca deis información de vuestras cuentas ni tarjetas por correo electrónico.

5.1.5. Peligro al abrir un archivo adjunto

Una de las vías más habituales de contagio de virus es a través del correo electrónico y, concretamente, a través de archivos adjuntos. Si vuestro antivirus detecta un archivo infectado, no lo abráis hasta que lo haya limpiado.

Hasta no hace mucho tiempo, sólo teníamos que desconfiar de los archivos ejecutables como EXE, COM, BAT,..., pero actualmente un virus puede hacerse pasar por casi cualquier tipo de archivo (JPG, DOC, PDF,...).

Para reducir los riesgos de infección por archivos adjuntos al correo electrónico, debemos tomar estas medidas:

- Disponer de un antivirus que revise automáticamente los correos y mantenerlo siempre actualizado.
- Sospechar de cualquier archivo con extensión EXE, COM, BAT, ZIP, SHS o PIF que no esperábamos recibir. Todos los archivos adjuntos al correo pueden contener virus pero estos tienen más posibilidades.
- Sospechar incluso cuando provienen de personas conocidas, puede que hayan suplantado su identidad. Ante la duda, es mejor llamar o escribir a la persona en cuestión para verificarlo antes de abrirlo.
- Antes de abrir un archivos adjunto, mejor descargarlo y analizarlo con nuestro antivirus.

5.2. MENSAJERÍA INSTANTÁNEA

5.2.1. Concepto y uso

La mensajería instantánea (MI) es un sistema que permite intercambiar mensajes entre dos o más personas en tiempo real, utilizando Internet. En los primeros programas de mensajería instantánea, cada letra era enviada después de escribirla, de esta manera las correcciones de los errores también se veían en tiempo real. Esto hacía que las conversaciones parecieran más una conversación telefónica que un intercambio de texto. En los programas actuales, habitualmente, se envía cada frase de texto una vez la hemos acabado de escribir. Además, se puede dejar mensajes, aunque la otra parte no esté conectada (estilo contestador automático) y se pueden enviar archivos.

El funcionamiento es muy sencillo: tenemos una lista de contactos (direcciones de correo), a las que hemos autorizado que sepan nuestro estado (conectado, desconectado, ocupado,...), aunque podemos falsearlo. Con los que estén disponibles podemos abrir una ventana de conversación.

Los clientes de mensajería instantánea más utilizados han sido Yahoo! Messenger, Windows Live Messenger (actualmente integrado en Skype) y Google Talk (sustituido actualmente por Hangouts). La última generación de los programas de mensajería nos permite utilizar webcam, micrófono o compartir juegos y aplicaciones.

Actualmente la mensajería instantánea se usa, cada vez más, en móviles y servicios. Los más conocidos son: Facebook Messenger, Skype, Line, Hangouts, Telegram y Whatsapp.

5.2.2. Vulnerabilidades de seguridad de la MI

Al igual que con el correo electrónico, con la mensajería instantánea estamos expuestos a cualquier ataque y, por lo tanto, debemos tomar precauciones:

- **Proteged vuestra identidad:** En los smartphones, normalmente, las aplicaciones de mensajería instantánea no piden usuario y contraseña cada vez que las utilizamos. Por lo tanto, en caso de pérdida o robo, la persona que se haga con el aparato puede enviar mensajes a todos nuestros contactos haciéndose pasar por nosotros. Para evitarlo, debemos activar una contraseña de bloqueo en el smartphone.

Si detectáis un comportamiento extraño de alguno de vuestros contactos, aseguraos de que es quien dice ser.

- **Utilizad antivirus en cualquier dispositivo:** Los archivos recibidos a través de aplicaciones de mensajería instantánea, sea cual sea el dispositivo, pueden contener virus (pueden ser archivos adjuntos o enlaces a alguna web).
- **Tened cuidado con los archivos multimedia:** Cuando recibimos un archivo multimedia a través de una aplicación de mensajería instantánea (fotos, vídeos,...) no sabemos su contenido hasta que lo reproducimos. Existe la posibilidad de que, sin saberlo, reproduzcamos contenidos ilegales; si los compartimos con otros usuarios, podemos estar cometiendo un delito.
- **No difundáis el número de teléfono móvil de otras personas** sin su consentimiento.
- **No facilitéis información privada:** No sabéis lo que pueden hacer con esa información.
- **Eliminad el historial de las conversaciones con frecuencia:** Evitaréis que, si alguien accede al dispositivo, pueda leerlas y obtener información vuestra.
- **Desconfiad de las redes WiFi públicas:** Si no están protegidas, podrían capturar vuestras conversaciones.
- **Mantened siempre actualizada la aplicación:** las actualizaciones pueden incorporar correcciones para los fallos de seguridad detectados.

6. GESTIÓN DE DATOS SEGUROS

6.1. COPIA DE SEGURIDAD DE LOS DATOS

Las copias de seguridad (backups) también es un aspecto que debe tenerse en cuenta a la hora de hablar de la seguridad: si no se tiene copia de respaldo de la información, puede ser que se pierda información valiosa por averías del disco duro, borrado accidental, infecciones víricas,...

Es necesario definir una política de copias de seguridad lo suficientemente robusta como para poder asegurar la recuperación de información en cualquier momento. Esta política de seguridad deberá contemplar entre otras cosas, la periodicidad de la realización de las copias (de nada sirve realizar una copia de seguridad esporádica, es necesario estudiar la automatización de las copias y el intervalo de tiempo que debe transcurrir entre una copia y otra), la definición de la información a salvaguardar (discriminar la información contenida en los discos seleccionando aquella que realmente se debe guardar), la ubicación de las copias (no puede guardarse las copias en un lugar que no sea seguro) y la comprobación del estado de las mismas (es necesario verificar periódicamente la validez de las copias).

6.1.1. Seguridad física de los dispositivos

Cuando hablamos de seguridad física nos referimos a los métodos usados para proteger el hardware y los datos almacenados ante amenazas que pueden provenir tanto del Hombre como de la naturaleza. Las principales amenazas son:

- Desastres naturales, incendios accidentales, instalación eléctrica (picos de tensión, cableado,...),...
- Ataques externos intencionados (robo, sabotaje,...).
- Ataques internos intencionados (robo, sabotaje,...).

Como es lógico, las posibles amenazas y las medidas de seguridad a tomar serán muy diferentes si se trata de un particular, de una pequeña empresa o de una multinacional, así como de la ubicación (para la prevención de desastres naturales) y del tipo de datos que se manejen.

Las copias de seguridad deberían:

- Estar, como mínimo, duplicadas.
- Estar almacenadas, físicamente, lejos de las instalaciones en las que se genera.
- Estar almacenadas en medios seguros.
- Ser realizadas y comprobadas a menudo.

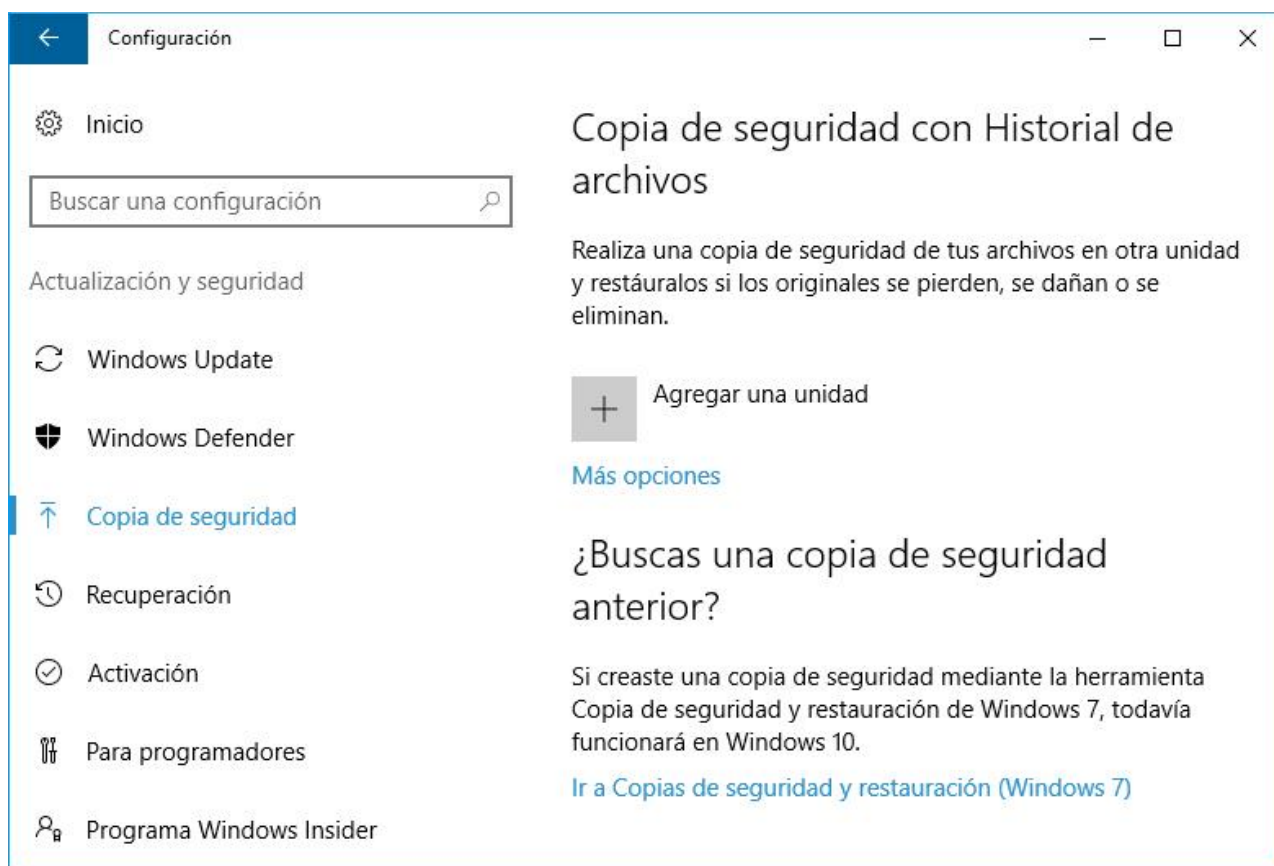
6.1.2. Herramientas de copia de seguridad en Windows

Windows nos ofrece 4 herramientas para la recuperación de datos:

- **Copia de seguridad de archivos:** Permite realizar copias de los archivos de datos para todos los usuarios del equipo. Podéis dejar que Windows elija qué se debe copiar o podéis seleccionar las carpetas, bibliotecas y unidades de las que realizar una copia de seguridad. Por defecto, las copias de seguridad se crean periódicamente, pero podréis cambiar la programación y crear manualmente una copia de seguridad en cualquier momento. Cada vez que se hace una nueva copia de seguridad, Windows comprueba qué archivos y carpetas son nuevos o han sido modificados y los añade a la copia de seguridad.
- **Copia de seguridad de imagen del sistema:** Permite crear una imagen del sistema. Una imagen del sistema incluye Windows, la configuración del sistema, los programas y los archivos. La imagen del sistema sirve para restaurar el contenido del equipo si la unidad del disco duro o el equipo dejan de funcionar. Cuando se restaura el equipo a partir de una imagen del sistema, la restauración es completa; no se pueden elegir que se restauren elementos individuales y se reemplaza todo. Aunque este tipo de copia de seguridad incluye los archivos personales, es recomendable realizar copias de seguridad periódicas de los archivos mediante Copias de seguridad de Windows para poder restaurar archivos y carpetas individuales cuando sea necesario.
- **Versiones anteriores:** Las versiones anteriores son copias de archivos y carpetas que Windows guarda automáticamente como parte de la protección del sistema. Podéis usarlas para recuperar archivos o carpetas modificados o eliminados por error, o dañados. Las versiones anteriores pueden ser útiles, pero no se deben considerar una copia de seguridad porque los archivos se reemplazan por nuevas versiones y no estarán disponibles si se produce un error en la unidad.
- **Restaurar sistema:** Permite restaurar los archivos de sistema del equipo a un momento anterior. Es una manera de deshacer los cambios del sistema realizados en el equipo sin que esto afecte a los archivos personales. Windows guarda periódicamente puntos de restauración en el equipo. Estos puntos de restauración contienen información acerca de la configuración del Registro y otra información del sistema que usa Windows. También podéis crear puntos de restauración manualmente.

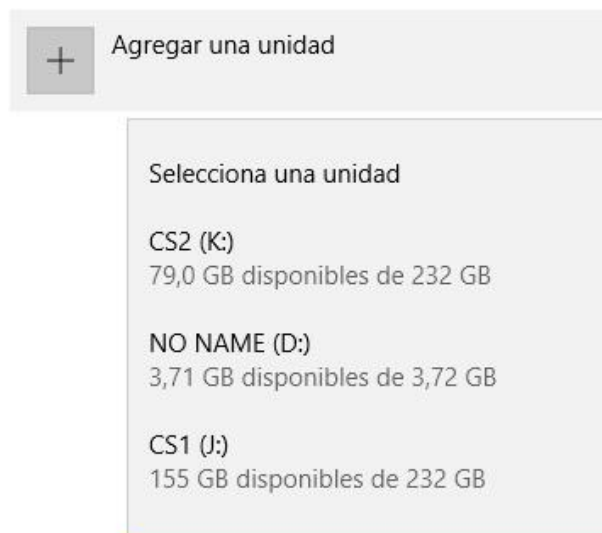
6.1.3. Hacer una copia de seguridad periódica

Para hacer una copia de seguridad periódica (con **Windows 10**) de los archivos de vuestro equipo, pedid **Configuración** (en el botón Inicio) y, en **Actualización y Seguridad**, clicad en **Copia de seguridad**:

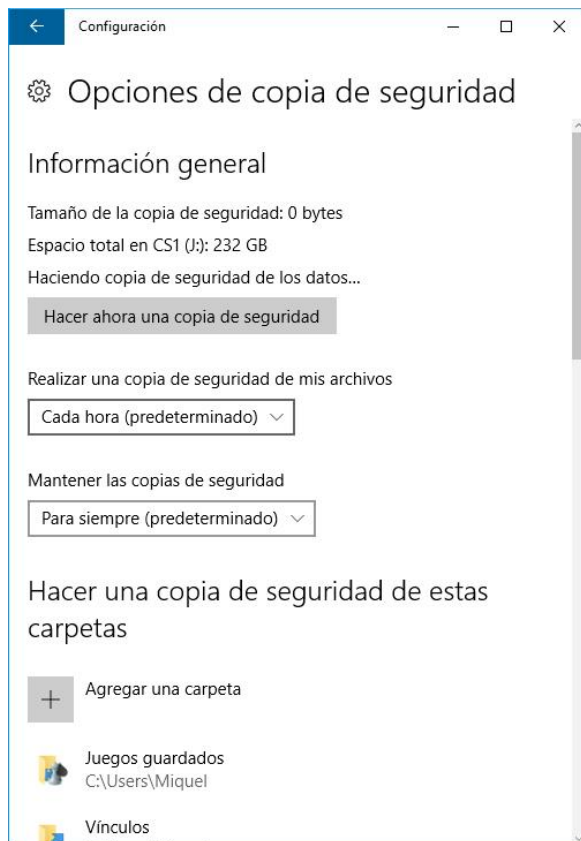


Escoged (con el botón **Agregar una unidad**) **dónde se guardará la copia** de seguridad. Puede guardarse en el mismo disco duro (no recomendable), en una unidad de CD/DVD, en un disco externo o en una unidad de red. Para un usuario particular, lo ideal es hacerlas en un disco duro externo. Si se trata de un ordenador del trabajo y se dispone de unidades de red, estas serán la ubicación más adecuada.

Este botón será sustituido por otro que indica que tenéis activada la copia de seguridad:



Clicad el enlace **Más opciones** para entrar en la ventana de configuración de la copia de seguridad:



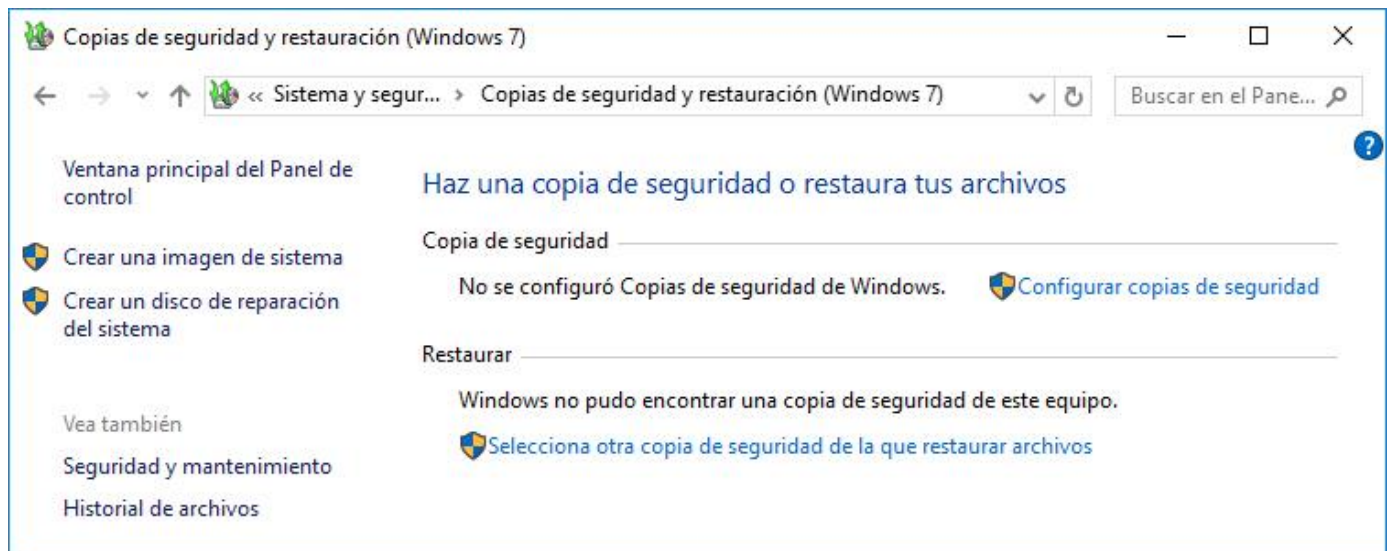
Para hacer la copia sólo hay que clicar el botón **Hacer ahora una copia de seguridad**.

Con la opción **Realizar una copia de seguridad de mis archivos**, podéis programar que haga automáticamente la copia cada cierto tiempo.

Con la opción **Mantener las copias de seguridad**, podéis indicar el tiempo que queréis que guarde las copias que irá haciendo.

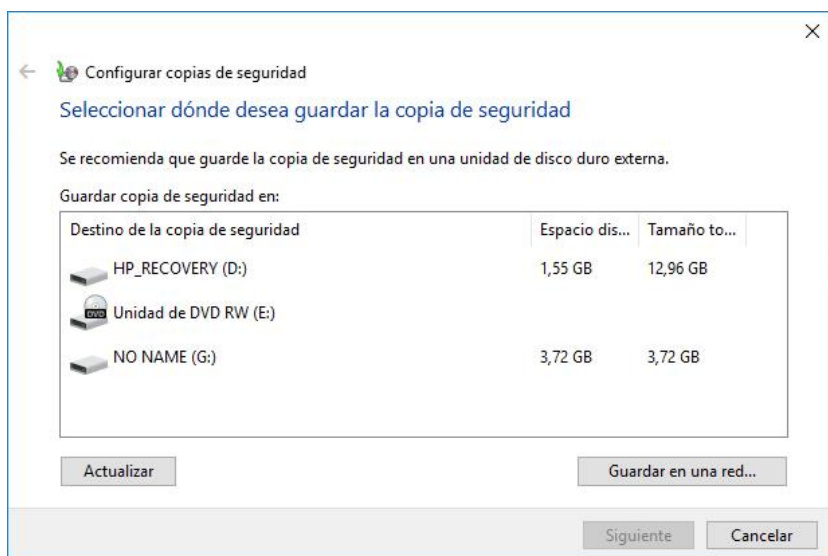
En el apartado **Hacer una copia de seguridad de estas carpetas**, se indica qué carpetas guardará en la copia de seguridad. Podéis añadir más carpetas (**Agregar una carpeta**) i quitar las que no queréis que se guarden (clicando sobre la carpeta aparece el botón **Quitar**).

También podéis configurar las copias de seguridad como se hacía con **Windows 7**, utilizando el **Panel de control**. Utilizaremos el **Panel de control Copias de seguridad y restauración (Windows 7) (Sistema y seguridad)**:



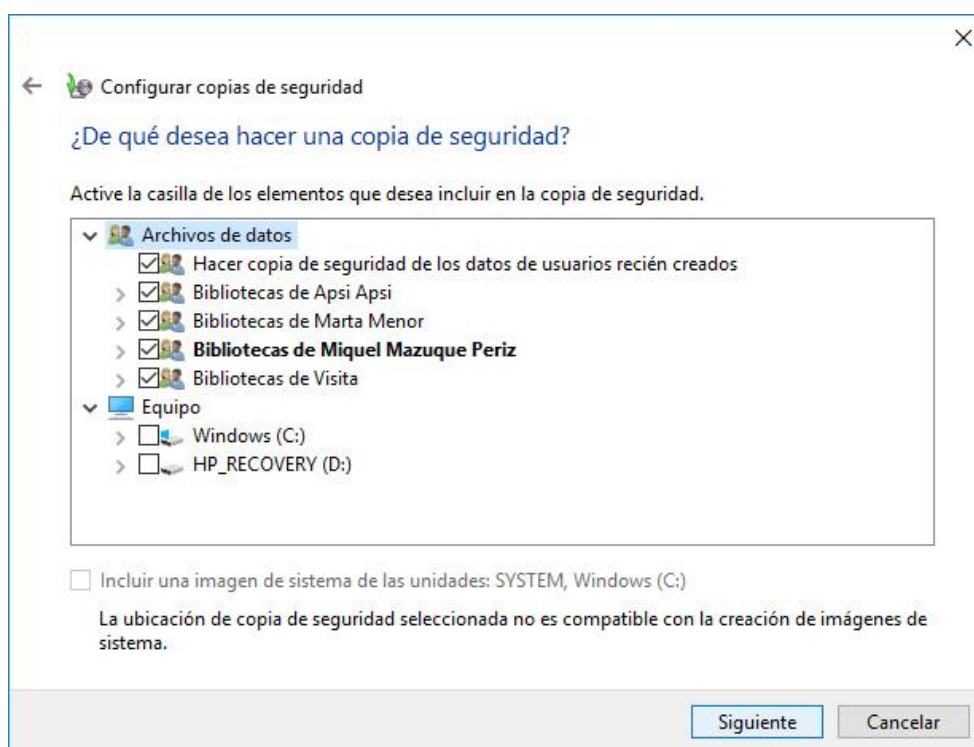
Si todavía no habéis hecho ninguna copia de seguridad del equipo, clicad en **Configurar copias de seguridad** y seguid los pasos del asistente:

1: Elegid dónde se guardará la copia de seguridad. Puede guardarse en el mismo disco duro (no recomendable), en una unidad de CD/DVD, en un disco externo o en una unidad de red. Para un usuario particular, lo ideal es hacerlas en un disco duro externo. Si se trata de un ordenador del trabajo y se dispone de unidades de red, éstas serán la ubicación más adecuada. En nuestro ejemplo utilizaremos un disco duro externo.



2: Indicad qué datos queréis guardar:

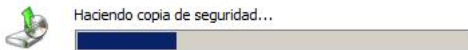
- **Dejar a Windows que elija (recomendado):** Es la opción más sencilla ya que guardará todos los archivos de las Bibliotecas, del Escritorio y de las carpetas predeterminadas de Windows (AppData, Contactos, Escritorio, Descargas, Favoritos, Vínculos, Juegos guardados y Búsquedas) de todos los usuarios que tengan una cuenta de usuario en el equipo.
- **Dejarme elegir:** Guardará los archivos de las carpetas que escojáis en la ventana que aparece al escogerla:



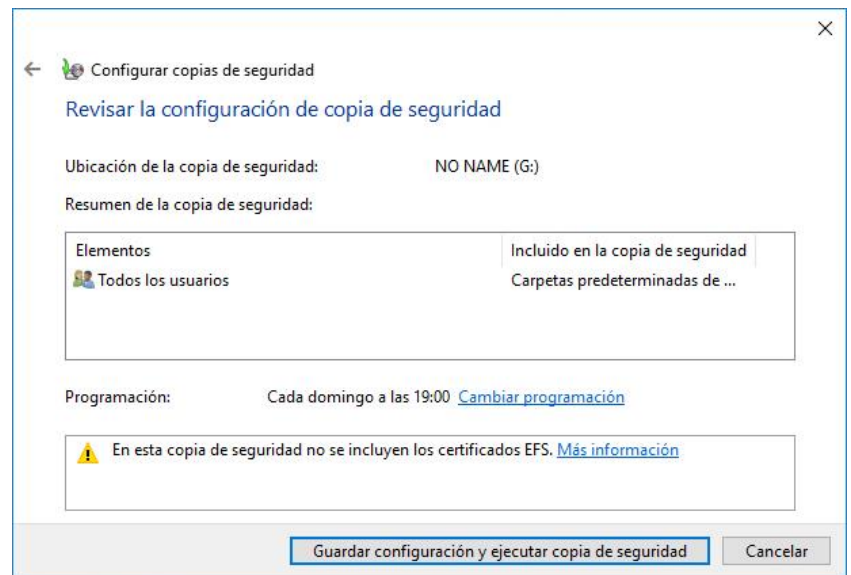
3: Mostrará qué datos van a guardarse

y podréis programar las sucesivas copias de seguridad (**Cambiar programación**).

Ya podéis clicar el botón **Guardar configuración y ejecutar copia de seguridad** y empezará a crear la copia de seguridad:



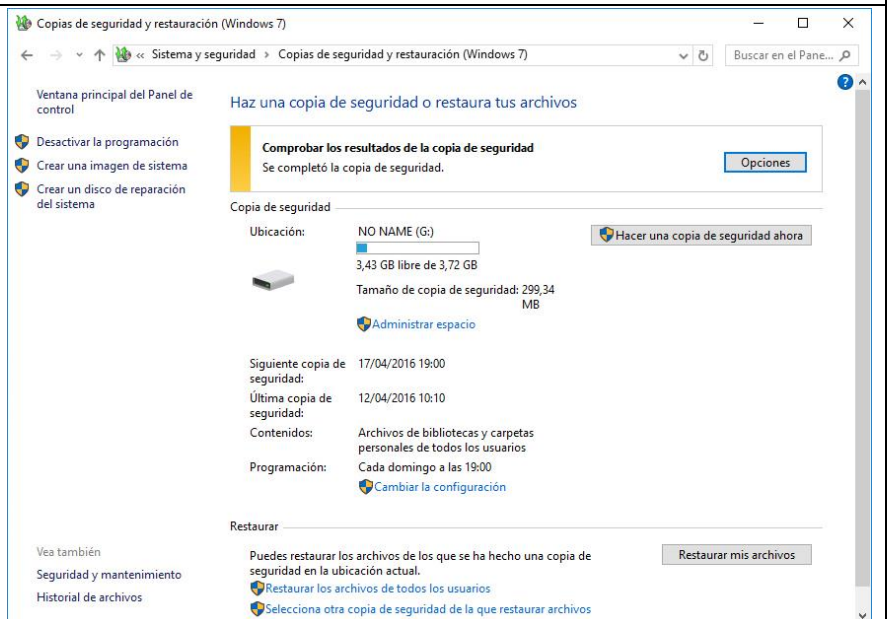
Si queréis **cancelar la copia**, antes de que acabe el proceso, clicad el botón **Ver Detalles** y, en la ventana de información que aparece, tendréis el botón **Detener copia de seguridad**.



A partir de ahora, al entrar al panel de control, mostrará los datos de la copia de seguridad programada.

Podéis modificarla con la opción **Cambiar la configuración**.

Si no queréis esperar hasta que realice la siguiente copia programada, podéis guardar una nueva copia manualmente, clicando el botón **Hacer una copia de seguridad ahora**.

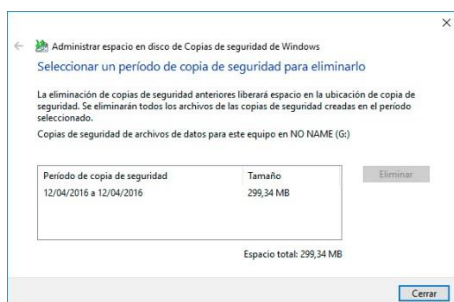
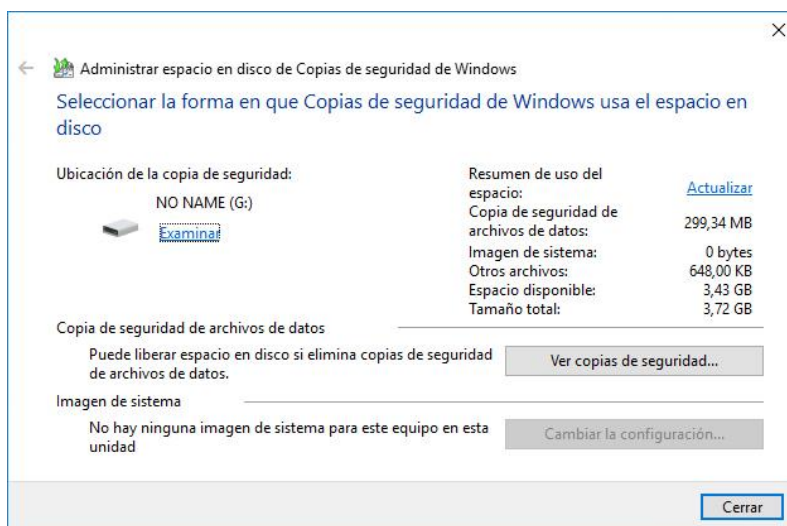


Podéis desactivar la programación automática de las copias con la opción **Desactivar programación**. De esta manera, sólo hará la copia cuando la pidáis con el botón **Hacer una copia de seguridad ahora**. Aparecerá la opción **Activar programación** para volver a activarla.

Si la copia la guardáis en un disco duro externo o en una unidad de red, tened presente que el día y hora programado para realizar la copia deberá estar conectado el disco duro al equipo o deberá estar conectado el equipo a la unidad de red. Al hacer las siguientes copias de seguridad, Windows comprobará qué archivos se han agregado o modificado desde la última copia de seguridad y, después, actualiza la copia de seguridad existente; esto permite ahorrar espacio en disco.

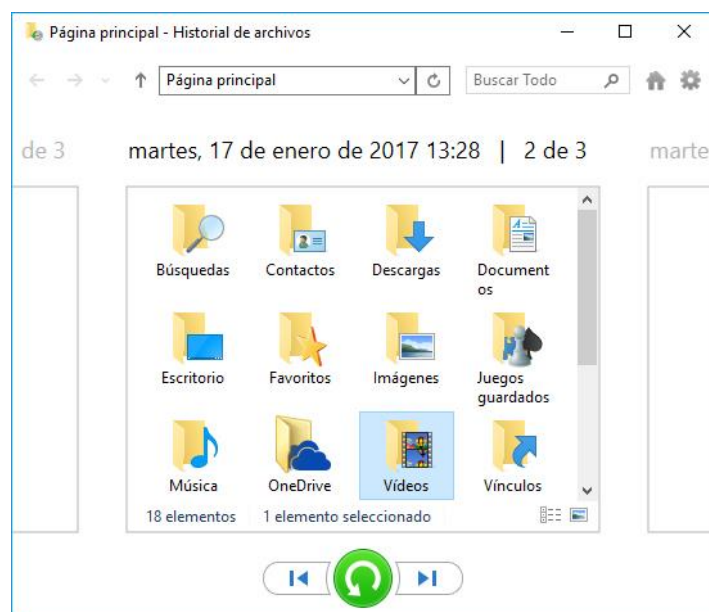
Podéis ver el espacio de disco usado para las copias de seguridad y el disponible, clicando la opción **Administrar espacio** del Panel de Control.

El botón **Ver copias de seguridad...** mostrará el listado de copias hechas hasta el momento y podréis eliminar las antiguas que ya no queráis conservar. Guardad siempre la más reciente.



6.1.4. Restaurar los datos respaldados

Si habéis hecho la copia de seguridad con la herramienta de Configuración de **Windows 10**, podéis recuperar los archivos guardados en la copia de seguridad hecha con la opción **Restaurar archivos desde una copia de Seguridad actual** que encontraréis al final de la ventana de configuración de copias de seguridad (**Inicio - Configuración - Actualización y Seguridad - Copia de Seguridad – Más opciones**).



Clicando el botón verde (**Restaurar en ubicación original**) recuperaréis los archivos. Si no queréis recuperar todos los archivos, podéis clicar en las carpetas para indicar cuáles queréis recuperar.

Los 2 botones de dirección os permiten escoger de qué copia de seguridad queréis recuperar los archivos.

Si lo queréis hacer como se hacía con **Windows 7**, utilizando el **Panel de control**, clicad el botón **Restaurar mis archivos** del Panel de control **Copias de seguridad y restauración (Windows 7)**. Si la copia contiene archivos de varios usuarios, podéis restaurar los archivos de todos los usuarios con la opción **Restaurar los archivos de todos los usuarios**. Os darán 3 opciones:

- **Buscar...**: Para restaurar archivos individuales, escribiendo su nombre. Podéis usar caracteres comodín como, por ejemplo, *.jpg para buscar todos los archivos JPG en la copia de seguridad.
- **Buscar archivos**: Para restaurar archivos individuales examinando el contenido de la copia de seguridad.
- **Buscar carpetas**: Para restaurar carpetas. Con esta opción no veréis los archivos que están en la carpeta.

Una vez indicado el archivo o carpeta a restaurar, preguntará si lo queréis en la ubicación original (donde estaba) o en alguna otra ubicación.

Si la restauración la pedimos después de reinstalar el sistema operativo, nos indicará que Windows no encontró ninguna copia de seguridad para este equipo. En este caso, debemos optar por la opción **Selecciona otra copia de seguridad de la que restaurar archivos**.

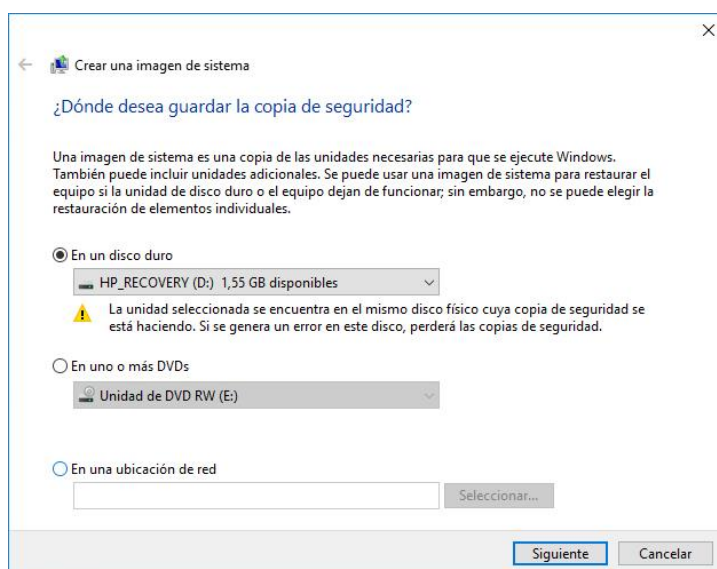
6.1.5. Crear una imagen del sistema

La función de copia de seguridad está diseñada para copiar sólo los documentos, no el sistema operativo ni las aplicaciones instaladas. Lo que más nos importa son los documentos que tenemos en nuestro ordenador pero, dado que en cualquier momento podemos tener algún problema (sobre todo a causa de los virus), también es conveniente disponer de la posibilidad de recuperar nuestro sistema operativo y las aplicaciones instaladas sin necesidad de volver a instalarlo todo. Esta función también la encontramos en el **Panel de control Copias de seguridad y restauración (Windows 7)** (apartado **Sistema y seguridad**): opción **Crear una imagen de sistema**.

En el asistente lo único que hay que hacer es escoger dónde guardar la imagen.

Una vez escogida la unidad, pedirá confirmación: clicad el botón **Iniciar la copia de seguridad**.

Si se guarda en un disco duro, debe estar formateado con el sistema de archivos NTFS.



Si guardáis las imágenes de sistema en una unidad interna o externa, o en CD/DVD, podéis mantener varias versiones de imágenes de sistema. En las unidades de disco duro internas y externas se eliminarán las imágenes

más antiguas cuando no haya suficiente espacio en la unidad. Podéis administrar las imágenes guardadas con la opción **Administrar espacio** del Panel de Control.

Si guardáis las imágenes de sistema en una ubicación de red, sólo podréis conservar la imagen de sistema más reciente de cada equipo. Las imágenes de sistema se guardan con el formato: *unidad\WindowsImageBackup\nombre de equipo*. Cuando hagáis una nueva imagen, sobrescribirá la existente.

También podéis pedir que haga una imagen del sistema a la vez que hace la copia de seguridad. En el segundo paso del asistente de creación de copia de seguridad (al escoger la opción **Dejarme elegir**) tenéis que activar la opción **Incluir una imagen de sistema de las unidades: SYSTEM, Windows (C:)**. No es aconsejable hacer la copia de seguridad y la imagen de sistema a la vez porque el proceso requiere mucho más tiempo y no hace falta hacer la imagen tan a menudo como las copias de seguridad. Mejor hacerlo por separado.

6.1.6. Restaurar el equipo a partir de una imagen del sistema

En cualquier momento podéis recuperar el sistema y las aplicaciones restaurando la imagen de sistema guardada.

¡Cuidado! Al restaurar el equipo a partir de una imagen de sistema, haréis una restauración completa; todos los programas, la configuración del sistema y los archivos se reemplazan por los de la imagen. Aseguraos de que el disco donde vais a restaurar la copia de seguridad sea de igual o mayor tamaño que el disco donde la hicisteis.

Para restaurar, pedid **Configuración** en el botón **Inicio** y, en **Actualización y Seguridad**, clicad en **Recuperación**:



Clicad el botón **Reiniciar ahora** y se abrirá el asistente con varias opciones:

- En la primera pantalla, escoged **Solucionar problemas**.
- En la segunda pantalla, escoged **Opciones avanzadas**.
- En la tercera pantalla, escoged **Recuperación de imagen del sistema**.
- Después, si tenéis cuentas de usuario, os pedirá que la escojáis y, para acabar, indicaréis dónde está la imagen.

Si no podéis acceder al Panel de control, podéis acceder a este asistente reiniciando el equipo. Mantened presionada la tecla **Mayúsculas** mientras se reinicia el equipo.

6.2. DESTRUCCIÓN SEGURA

La destrucción efectiva de la documentación digital o impresa que genera una empresa, sobre todo cuando contiene datos de carácter personal, ha de realizarse correctamente para no incumplir la Ley Orgánica de Protección de Datos (LOPD). Esta ley obliga, en ciertos casos, a la eliminación definitiva de la documentación que contiene información confidencial.

En el caso de la **documentación impresa** no basta con tirar los documentos a la basura o rasgar simplemente el papel. La ley indica que se dispone, básicamente de tres sistemas:

- **Subcontratar** a una empresa especializada en destrucción de papel.
- **Triturar** el papel con una trituradora de papel.
- **Quemar** el papel.

En el caso de la **documentación digital**, existen distintos métodos de destrucción de la información: desmagnetización, destrucción y sobre-escritura, que pueden ser más adecuados en función del tipo de dispositivo (magnético, óptico o electrónico).

6.2.1. ¿Qué datos hay que eliminar de dispositivos de manera permanente?

Los datos susceptibles de ser eliminados se clasifican en 3 niveles de seguridad:

Nivel Alto:

- De ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico.
- Recabados con fines policiales sin consentimiento de las personas afectadas.
- Derivados de actos de violencia de género.

Nivel Medio:

- Relativos a la comisión de infracciones administrativas o penales.
- Que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito).
- De Administraciones tributarias y que se relacionen con el ejercicio de sus potestades tributarias.
- De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros.
- De Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias.
- De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Que ofrezcan una definición de la personalidad y permita evaluar determinados aspectos de la misma o del comportamiento de las personas.

- De los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.

Nivel Básico:

Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesorio, que no guarden relación con la finalidad del fichero.
- Los ficheros o tratamientos contengan datos de salud que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez con motivo del cumplimiento de deberes públicos.

Encontraréis información en la **Guía del Documento de Seguridad** de la **Agencia Española de Protección de Datos**:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

6.2.2. Diferencia entre eliminar y destruir datos de manera permanente

Eliminar o borrar los datos consiste simplemente en hacer que los datos ya no sean visibles para la aplicación o el usuario final. Dependiendo de la tecnología de que se trate, los datos pueden ser fácilmente recuperados o necesitar de la intervención de un experto. La **destrucción** de datos consiste en volver los datos completamente ilegibles, incluso para un profesional.

6.2.3. Métodos para destruir de manera permanente datos digitales

Existen diferentes métodos dependiendo de en qué grado se pretenden destruir los datos:

- **Sobreescritura:** Podemos usar software que sobrescribe los datos borrados substituyéndolos por secuencias de unos y ceros. Pueden utilizarse para dispositivos magnéticos (discos duros), o electrónicos (memorias Flash USB,...). Un ejemplo es **Eraser**. Eraser permite seleccionar el método de borrado de datos (varios niveles de seguridad), se puede utilizar con discos duros, pendrives, tarjetas de memoria,... y permite programar borrados de una forma sencilla.
- **Desmagnetización:** La desmagnetización bombardea la unidad con un campo magnético lo suficientemente potente como para que todos los bits de la cinta o disco se alineen de determinada manera, quedando todos los datos borrados. Hay que tener en cuenta que cada cinta, tipo de cinta y unidad de disco requieren una unidad de desmagnetización de potencia distinta para lograrlo.
- **Destrucción:** Es el equivalente electrónico de una máquina trituradora.

Webs consultadas:

Agencia Española de Protección de Datos (Gobierno de España): <https://www.agpd.es/>

BBC: <http://www.bbc.com/>

Expertos en sistemas: <http://www.expertosensistemas.com/>

Geekland (Blog de tecnología): <http://geekland.eu/>

Gizmodo: <http://es.gizmodo.com/>

Instituto Nacional de Ciberseguridad de España (Gobierno de España): <https://www.incibe.es/>

Internet Security Auditors: <http://www.isecauditors.com/>

Kaspersky: <http://www.kaspersky.es/>

Laboratorio de Redes y Seguridad (Univ. Nacional Autónoma de México): <http://redyseguridad.fi-p.unam.mx/>

Maestros del web: <http://www.maestrosdelweb.com/>

Microsoft: <http://www.microsoft.com/>

Ministerio de Educación (Argentina): <http://coleccion.educ.ar/>

Ministerio de Educación, Cultura y Deporte (Gobierno de España): <http://www.mecd.gob.es/portada-mecd/>

Network World: <http://www.networkworld.es/>

Oficina de Seguridad del Internauta (Instituto Nacional de Ciberseguridad): <https://www.osi.es/>

Panda: <http://www.pandasecurity.com/>

PC Actual: <http://www.pcactual.com/>

PC Webtips: <http://www.pcwebtips.com/>

Portal Administración Electrónica (Gobierno de España): <http://administracionelectronica.gob.es>

Protección Online: <http://www.protecciononline.com/>

SearchDataCenter: <http://searchdatacenter.techtarget.com/>

Security in a box: <https://info.securityinabox.org/>

Universidad Carlos III: <http://www.uc3m.es>

WikiHow: <http://es.wikihow.com/>

Wikipedia: <https://www.wikipedia.org/>

Wordpress.com: <https://protejete.wordpress.com/>