SEGURIDADE

Entendemos por seguridad informática el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad.Tenemos que ser conscientes de que las pérdidas de información no pueden venir sólo de ataques externos sino que pueden producirse por errores nuestros o por accidentes o averías en los equipos.

El elemento clave de un sistema de información son los datos y hay dos principales amenazas externas al software y a los datos:

2.1 Código malicioso (malware)

2.2 Ingeniería social

2.1 Código malicioso (malware)

El código malicioso o malware, es un programa que tiene como objetivo introducirse y hacer daño en un ordenador sin que el usuario lo note. Entre sus objetivos podemos señalar:

- Robar información, datos personales, claves, números de cuenta.
- Crear redes de ordenadores zombis, denominadas también botnet, para ser utilizadas en el envío masico de spam, phising, realización de ataques de denegación de servicio.
- Cifrar el contenido de determinados archivos para solicitar el pago de una cantidad para solucionarlo (ransomware).

Hay diferentes tipos de malware entre los que podemos destacar los siguientes:

Virus

Es un código malicioso que tiene como objetivos alterar el funcionamiento de un ordenador sin el conocimiento del usuario. Por lo general incorporan código infectado en archivos ejecutables activándose los virus cuando se ejecuta este archivo. En ese momento el virus se aloja en la memoria RAM y se apodera de los servicios básicos del sistema operativo. Cuando el usuario ejecuta otro archivo ejecutable, el virus alojado en la RAM lo infecta también para ir de esta manera replicándose.

Gusanos

Es un tipo de virus. La principal diferencia entre gusano y virus es que el gusano no necesita la intervención humana para ser propagado, lo hace automáticamente, no necesita alojarse en el código anfitrión, se propaga de modo autónomo, sin intervención de una persona que ejecute el archivo infectado. Suelen apropiarse de los servicios de transmisión de datos para controlarlo. Por lo general los gusanos consumen mucha memoria provocando que los equipos no funcionen adecuadamente. Uno de los sistemas que utiliza el gusano para propagarse es enviarse a sí mismo mediante correo electrónico a los contactos que se encuentran en el ordenador infectado.

Troyanos

Son programas aparentemente inofensivos que tienen una función no deseada. Son realmente un programa dañino con apariencia de software útil que puede acabar siendo una gran amenaza contra el sistema informático. Ejemplos de virus que se pueden identificar como troyanos serían:

Puertas traseras (backdoors): Modifican el sistema para permitir una puerta oculta de acceso al mismo de modo que el servidor toma posesión del equipo como si fuese propio lo que permite

tener acceso a todos los recursos, programas, contraseñas, correo electrónico, unas veces en modo de vigilancia y otras para modificar la información y utilizarla con fines no licítos.

Keyloggers: Almacenan todas las pulsaciones del teclado que realiza el usuario. Se utilizan normalmente para robar contraseñas.

Spyware: Envía información del sistema el exterior de forma automática. Es un código malicioso que, para instalarse en un ordenador, necesita la participación de un virus o troyano, aún que también puede estar oculto en los archivos de instalación de un programa normal. Su cometido es obtener información de los usuarios que utilizan ese ordenador. E objetivo más leve y más común es aportar los datos a determinadas empresas de márketing online que, con posterioridad y por diferentes medios, correo electrónico, pop-ups, enviarán publicidad al usuario sobre los temas que detectaron que les podían interesar.

Estos programas espía pueden indagar en toda la información existente en el equipo, como listas de contactos, información recibida, enviada, por ejemplo el dni, números de tarjetas de crédito, cuentas bancarias, domicilios, teléfonos, software que tiene instalado, direccións ip, servidores de internet que utiliza, páginas web que visita, tiempo de permanencia en un sitio web, etc. Por otra parte, el spyware puede servir como sistema de detección de delitos cometidos a través de internet, es muy representativa la utilización por la Policía española de código malicioso incorporado a fotos de menores que permite identificar casos de corrupción de menores y pederastia.

Adware: Programas de publicidad que muestran anuncios, generalmente mediante ventanas emergentes o páginas del navegador.

Los equipos se pueden infectar si ejecutan algún programa no adecuado, con código maligno, generalmente recibido por correo electrónico como adjunto al mismo o bien descargado de internet. A veces también es posible que sea instalado directamente en el equipo por una persona con acceso físico al mismo.

Bot malicioso

También son conocidos como robot web, bot es la simplificación de robot, se trata de un programa que pretende emular el comportamiento humano. Hay bots con fines lúdicos, que buscan mantener un chat con una persona, ser contrincante en un juego o de rastreo como los que usan los buscadores google o yahoo que tienen como finalidad detectar el movimiento que se produce en los sitios webs a los que enlazan y ofrecen las novedades en las búsquedas de los usuarios. Los bots maliciosos son realmente troyanos de puerta trasera, con la particularidad de que se instalan en los equipos vulnerables mediante el sistema de rastreo en internet. Una vez infectado el equipo envía una señal a su creador y pasa a formar parte de una botnet o red de bots.

A los bots se les denomina zombis, pues cumplen las órdenes de los ciberdelincuentes que los crearon. Así pueden reenviar spam y virus, robar información confidencial o privada, envíar órdenes de denegación de servicio en internet o hacer clic automáticamente en anuncios publicitarios en la página web del ciberdelincuente que pagan por clic efectuado

Virus de macro

También se denominan macro virus, son un subtipo de virus que es creado en macros inscritas en documentos, páginas web, presentaciones, … Si el ordenador de la víctima abre un documento infectado la macro pasa a la biblioteca de macros de la aplicación que ejecuta, con lo que la macro acabará ejecutándose en los diferentes documentos que se abran con esta aplicación. Los resutados de ejecución de este virus son muy variados, desde auto-enviar un documento por correo electrónico a una dirección definida en la macro hasta realizar cálculos matemáticos erróneos.

2.2 Ingeniería social

Es la manipulación inteligente de la tendencia natural de la gente a confiar. Consiste en obtener información a través de las personas que la utilizan. No es necesario recurrir a programas complejos, código malicioso o estrategias para entrar en sistemas informáticos utilizando puertas traseras aprovechando la vulnerabilidad del software o del sistema operativo. Utiliza los más antiguos métodos de engaño y timo, pero utilizados a nivel informático con la máxima de que el ser humano es el eslabón más débil de la cadena, cuando nos referimos a seguridad de los sistemas de información.

El método principal es el correo electrónico, las cadenas de correos buscan obtener direcciones de correo electrónico para poder enviarles spam, un correo de este tipo se multiplica de forma exponencial con lo que más tarde o más temprano lo vuelve a recibir pero averiguando cientos de direcciones de email. A veces pueden buscar colapsar los servidores de correo o los correos millonarios como la lotería de los nigerianos que se comprometían a entregarte una gran cantidad de dinero si le proporcionabas una cuenta para meter la cantidad ganadora.

Dentro de la ingeniería social está el método conocido como **phishing**, palabra parecida al término inglés de pescar fishing pero con la p de password.

Puede llegar a través de un correo electrónico de gente desconocida o de sitios webs de poca confianza pero en ocasiones parece que proviene de contactos conocidos, bancos o organismos oficiales. Por tratarse de correos de fuentes de confianza, aumentan las posibilidades de que la víctima llegue a caer en la trampa.

Un ejemplo típico es el de que la víctima recibe un correo electrónico de su director de su oficina bancaria en el que se le comunica que el nuevo método de acceder a banca electrónica es pulsando sobre un enlace que le envía realmente a una web fraudulenta con apariencia similar a la real. El objetivo es hacerse con el nombre de usuario y la contraseña real para poder operar con ellas en su nombre.

Ejemplos de phising:

2.3 Medidas de seguridad

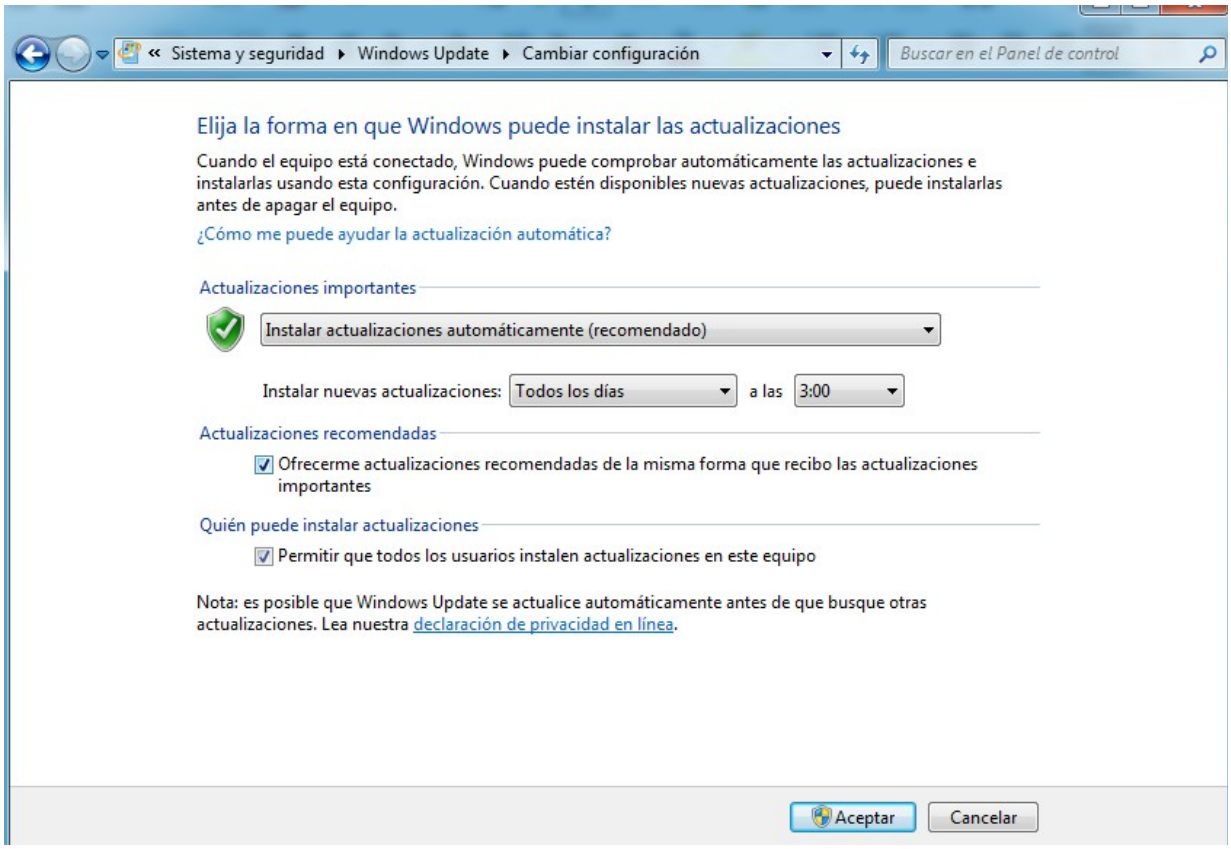
Para proteger nuestros sistemas informáticos tenemos dos tipos de medidas, de seguridad activa y de seguridad pasiva. Las medidas de seguridad activa buscan evitar daños e intrusiones en los equipos, en su software y en la información que contienen. Un ejemplo sería un antivirus. Por otro

lado las medidas de seguridad pasivas son las destinadas a minimizar el daño cuando la avería o la entrada de malware ya se ha producido (ej: la realización de copias de seguridad). Haciendo una analogía con la seguridad en el automóvil la revisión de los frenos y los neumáticos es una medida de seguridad activa porque se realizan para evitar que se produzca el accidente y el airbag es una medida de seguridad pasiva porque interviene para minimizar el daño cuando ya se ha producido el accidente.

A continuación vamos a exponer diferentes técnicas que ayudarán a proteger nuestros sistemas.

1. Tener el sistema operativo actualizado y programadas las actualizaciones automáticas

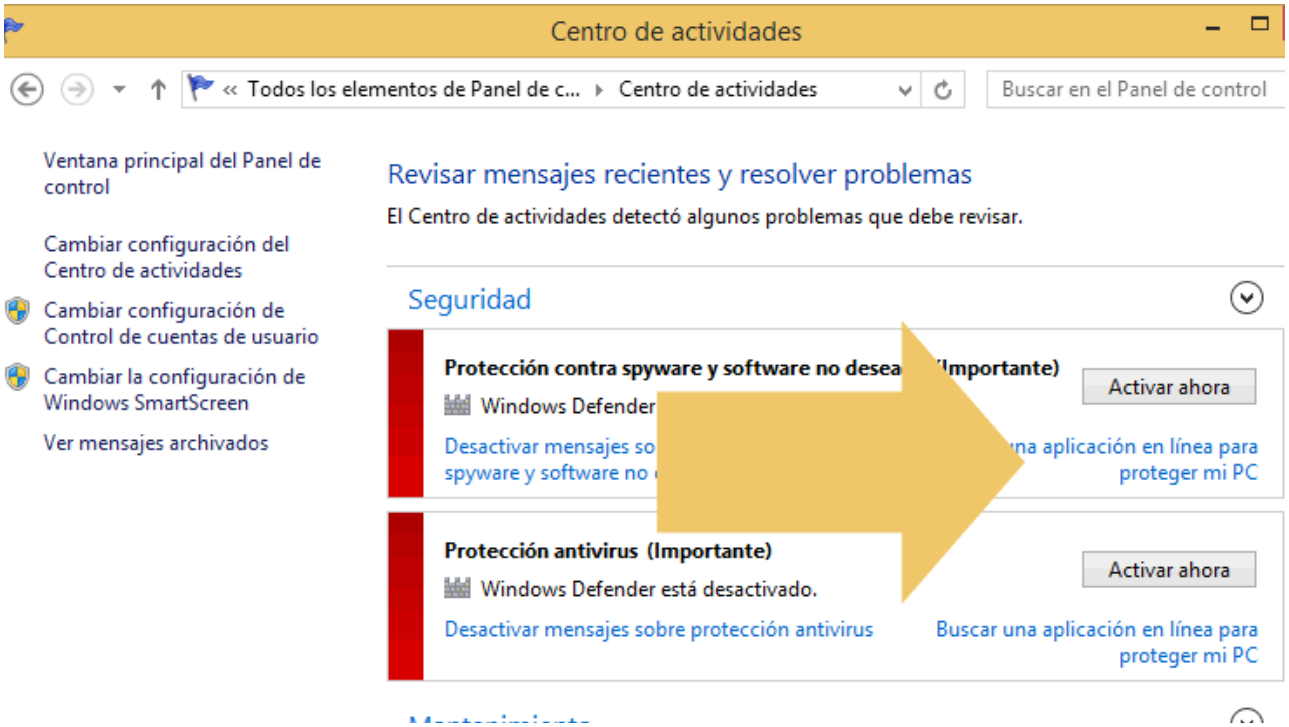
El ataque del último virus informático tipo ransomware (secuestro de datos) que actuó a nivel mundial fue posible porque entró en equipos que no tenían su sistema operativo actualizado. Las empresas sacan periódicamente parches que solucionan los problemas informáticos que se van detectando, por lo que es fundamental que se actualicen automáticamente. Para ello por ejemplo en windows sólo tenemos que ir al panel de control en la categoría de Sistema y seguridad – Windows update – (menú de la izquierda) Cambiar configuración y allí escoger instalar actualizaciones automáticamente y marcar las pestañas de actualizaciones recomendadas y permitir que todos los usuarios puedan instalar actualizaciones en el equipo.



2. Tener un programa antivirus con protección antispyware configurado con actualizaciones automáticas

El antivirus es un programa cuya finalidad es detectar, impedir la ejecución y eliminar software malicioso como virus informáticos, gusanos, espías, etc... Los antivirus pueden estar en **estado residente**, es decir análisis continuo de la información en movimiento entrando y saliendo (es la opción recomendada y es la que tiene que estar activada) o en estado de **análisis completo pasivo** con el cual se realizarán análisis completo del sistema de forma periódica o a decisión del usuario.

Windows 10 tiene un antivirus propio (Defender) que mejora considerablemente las prestaciones de los antivirus de las versiones de windows anteriores por lo que puede ser suficiente. Para activarlo vamos a Panel de control – Centro de actividades – Seguridad y activar la protección contra virus y contra spyware.



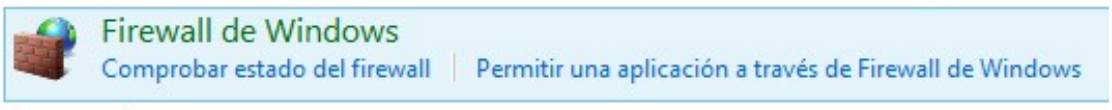
Entre los antivirus gratuitos destacan el AVG (http://www.avg.com/es-es/homepage) y el AVAST (https://www.avast.com/es-es/index)

3. Tener el firewall (cortafuegos) activado

El firewall es el software o hardware cuya finalidad es permitir o prohibir la comunicación entre las aplicaciones de nuestro equipo y la red, así como evitar ataques intrusos desde otros equipo al nuestro mediante el protocolo TCP/IP. Es una barrera de protección entre nuestro equipo y el exterior (internet) . Controla el acceso de entrada y salida, filtra las comunicaciones, registra los eventos y genera alarmas.

Si alguna aplicación desea establecer conexiones periódicas con nuestro equipo desde internet sin pedir permiso para cada conexión, deberá instalarse y ser reconocida como **excepción** en el firewall.

Para activarlo en windows 8 vamos a Panel de control – (Categoría) Sistema y seguridad – Firewall de windows – Activarlo.

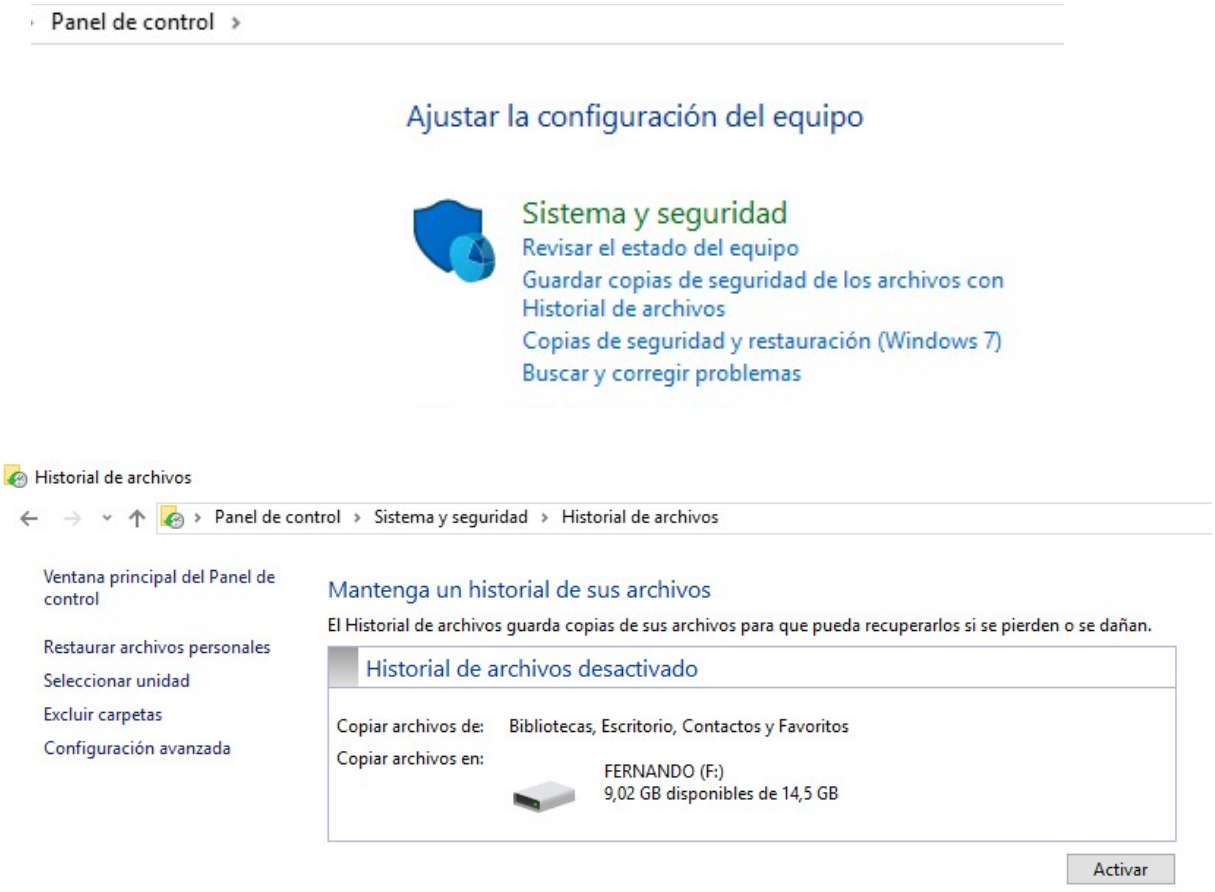


4. Realizar copias de seguridad

La realización periódica y sistemática de copias de seguridad es una de las tareas de seguridad más importantes , dado que en caso de pérdida de información por cualquiera de los motivos anteriormente citados (averías, roturas , virus , caídas) los daños reales serán mínimos, salvo la pérdida de tiempo que conlleve la restitución de lo perdido.

La copia de seguridad puede hacerse a muchos niveles dependiendo de qué es lo que intentemos proteger, desde un solo archivo hasta una partición de disco duro, o incluso el disco duro completo incluyendo los diferentes S.O. que podamos tener en sus particiones, los drivers y el resto del contenido . La elección del tipo de copia que deseamos hacer dependerá de los intereses del usuario y por lo general para uso particular la solución más sencilla es la de hacer copia de ciertos archivos de tipo personal, dado que esta es rápida y fácil de copiar y los programas del equipo son en principio más fácilmente recuperables.

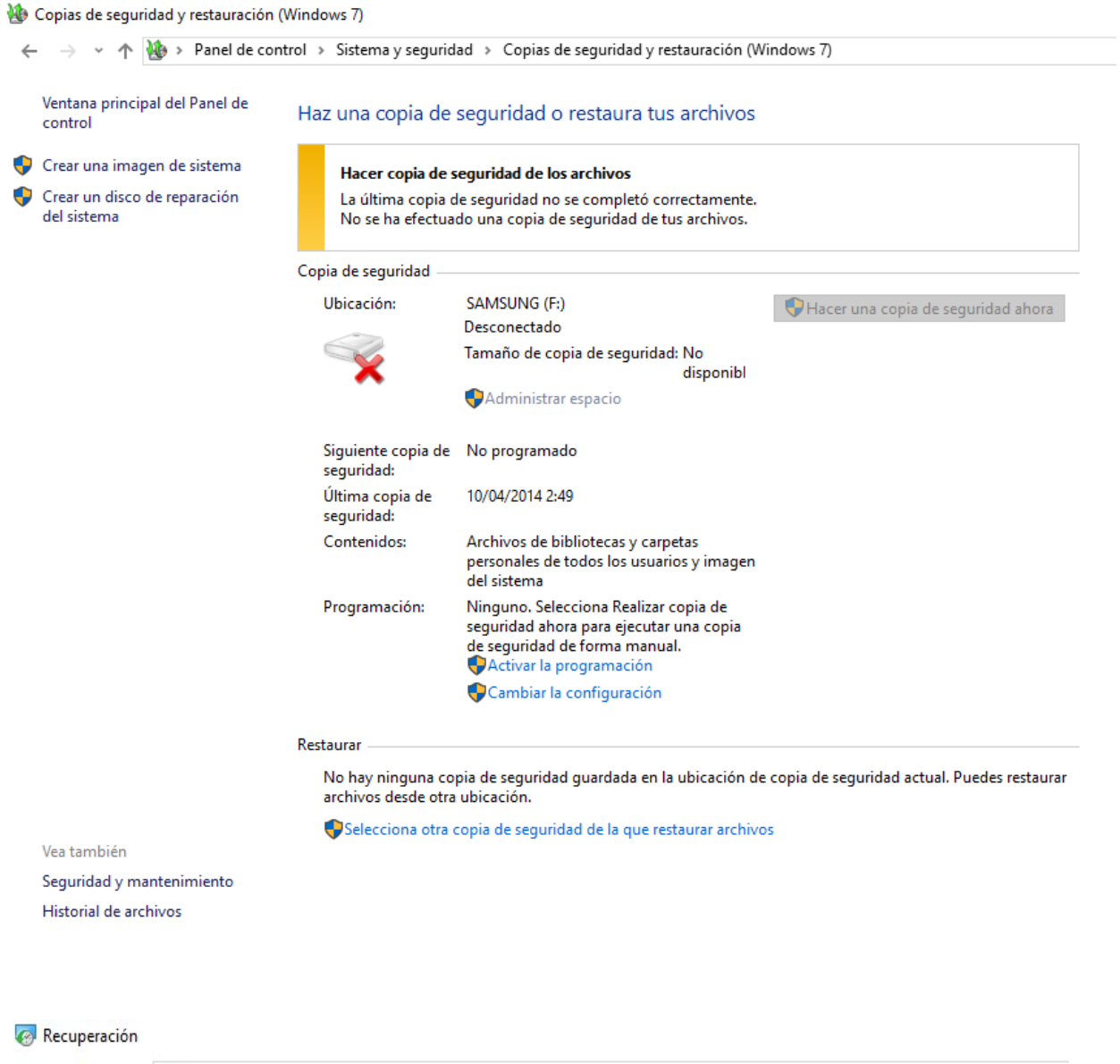
Las últimas versiones de windows nos permiten hacer copias de seguridad de unas carpetas determinadas (Bibliotecas (Documentos, imágenes, música, vídeos), Escritorio, Contactos y Favoritos) en Panel de control – Sistema y seguridad (categoría) – Guardar copias de seguridad de los archivos con Historial de archivos y luego restaurarlas pinchando en la siguiente ventana en Restaurar archivos personales. Debes tener una memoria externa en un usb para realizarla.

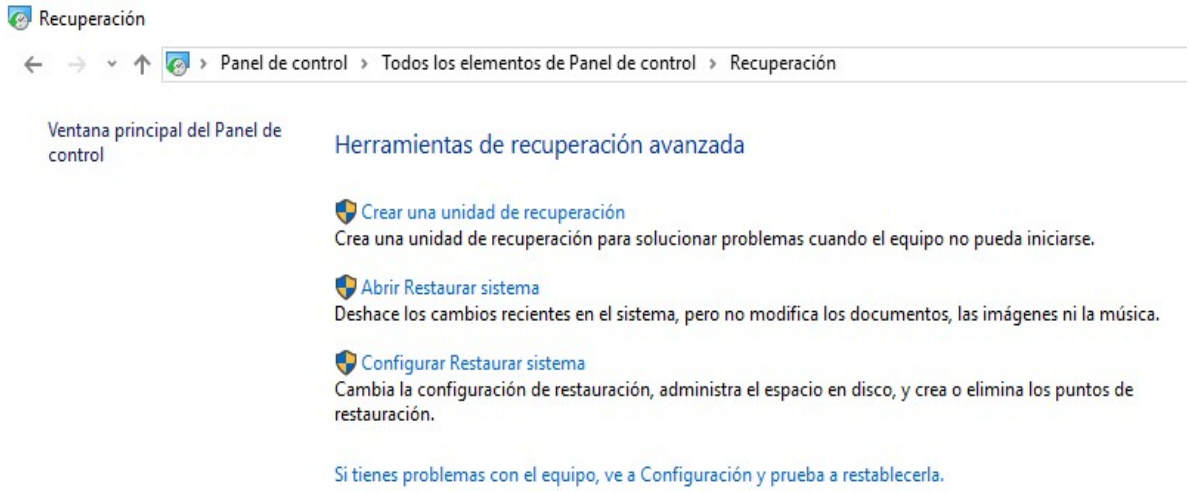


Se puede realizar una copia de todos los archivos no sólo las carpetas anteriores pinchando en Copias de seguridad y restauración (Windows 7). En este caso la copia se puede guardar en el disco duro, no es obligatorio hacerlo en una memoria externa conectada a un puerto usb.

También nos permite hacer una imagen del sistema (en la que queda guardado absolutamente todo: archivos, programas y sistema operativo). Hoy en día muchos ordenadores traen una imagen del sistema en una partición del disco duro. En caso de colapso total de tal forma que no

aparezca el menú de arranque y de restauración para restaurar esta imagen de fábrica o una creada por nosotros necesitaremos un CD o un pendrive desde el que arrancaremos cuando deseemos emplear la imagen del sistema modificando el orden de arranque (boot) en la BIOS. Para crearlo iríamos a Panel de Control – Recuperación – Crear una unidad de recuperación.





Estas cuatro medidas anteriores son de las más importantes en cuanto a seguridad, pero hay otras técnicas relacionadas con la seguridad que también nos pueden ser muy útiles, son las siguientes:

a) **Proteger archivos y carpetas con contraseña**: Tanto en Libre Office como en Microsoft Office a la hora de guardar un archivo aparece la opción de guardar con contraseña, de tal forma que quien no la tenga no podría abrir el archivo.
La protección de carpetas con contraseña la podemos realizar con el 7-zip, a la hora de crear la carpeta escogemos la opción de añadir al archivo… y ahí podemos meter la contraseña.

b) **Archivos ocultos:** Mediante esta herramienta podemos conseguir que las carpetas que seleccionemos y los archivos que estas contienen no se muestren en los navegadores de archivos ni en el escritorio, dificultando el acceso a las mismas.

El SO oculta algunos de sus directorios de forma predeterminada para de esta forma evitar el borrado o manipulación accidental de estos archivos fundamentales para el funcionamiento del sistema y que además carecen de utilidad para el usuario. Para ocultar una carpeta, pinchando con el botón derecho y yendo a propiedades marcamos la pestaña de oculto. Para verlo si recordamos la ruta poniéndola en el explorador de windows aparecerá, sino iríamos a Panel de Control – Apariencia y personalización – Mostrar todos los archivos y carpetas ocultas – Ver – Mostrar archivos, carpetas y unidades ocultas.

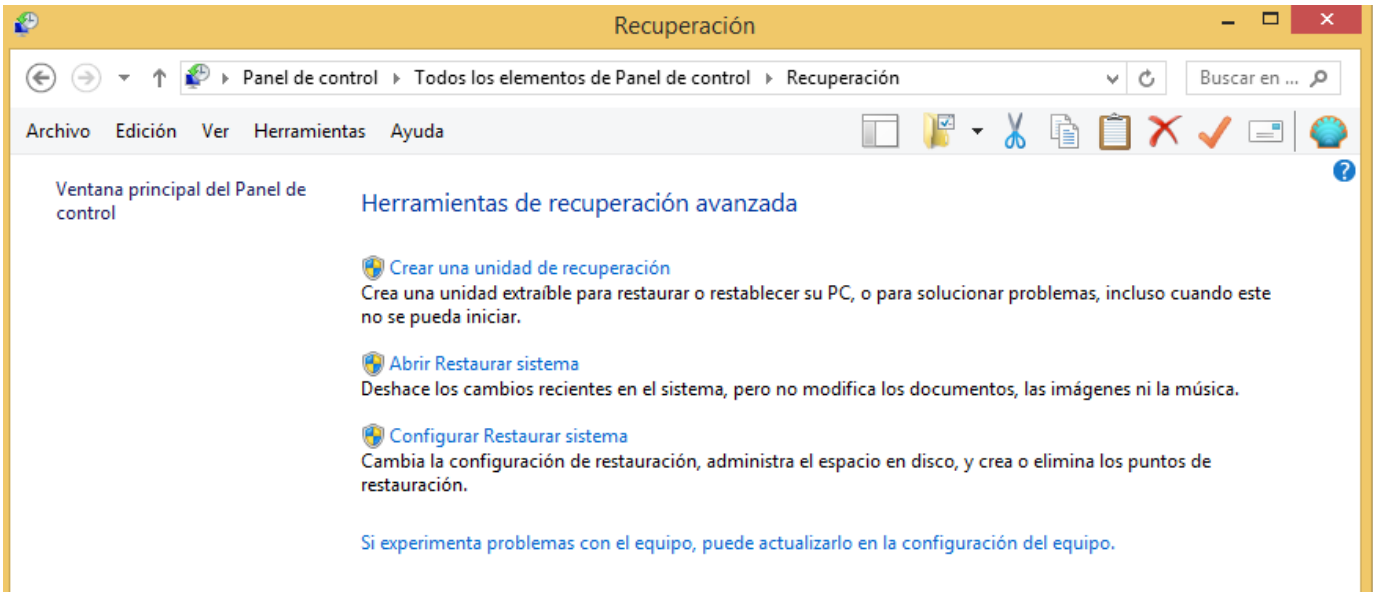
c) **Congelación de software**: Los programas "congeladores" son un software del tipo "reinicie y restaure". Basicamente, un programa congelador es aquel que se encarga de impedir que todo cambio que realices en la computadora (agregar programas, guardar archivos, etc), se apliquen o guarden. Una vez que reinicias la computadora, todo lo que hayas hecho se borra, y la computadora vuelve al estado inicial al que estaba al activar el programa congelador. se puede congelar sólo la particion del disco duro donde está el sistema operativo, teniendo la otra unidad libre para guardar lo que desees sin que se pierda (D:). El software de congelación de pago más conocido es deepfreeze y el gratuito es toolwiz time freeze (http://www.toolwiz.com/lead/toolwiz_time_freeze/)

d) **Recuperación de archivos**: Hay programas que basándose en que la información eliminada de cualquier unidad de memoria no es realmente borrada en ese instante, son capaces de recuperar archivos que hayamos eliminado de la papelera de reciclaje e incluso en ocasiones de unidades formateadas. La efectividad de estos programas es en ocasiones baja , por lo que a veces es necesario probar la recuperación con distintos “ Recuperadores “ . Además algunos de estos programas son capaces de “Reparar Archivos” , o recuperarlos cuando hay parte de ellos que realmente ha sido borrada, por lo que en ocasiones también se emplean para reparar archivos dañados . El más popular es el programa Recuva. (https://www.piriform.com/recuva)

e) **Particiones**: Pese a que la posibilidad de particionar unidades de memoria no es en sí un elemento de seguridad, puede ser usada como tal si se emplean dichas particiones para almacenar información duplicada, desde simples archivos hasta imágenes completas de disco para ejecutar recuperaciones completas del sistema, incluyendo incluso drivers y programas. De esta forma y como cada partición tendrá su formato, si una de las particiones se ve dañada, la otra u otras no tendrían porque verse afectadas y se podría recuperar la información. Lo más usual en Windows es tener una partición donde residen el S.O. y otros programas de aplicación, y otra partición para almacenar ficheros, archivos, datos, etc...Se pueden realizar y eliminar particiones desde el propio sistema operativo, pero es una operación que hay que realizar con mucho cuidado porque es relativamente fácil perder toda la información, por lo que antes de realizarla se debe ejecutar una copia de seguridad.

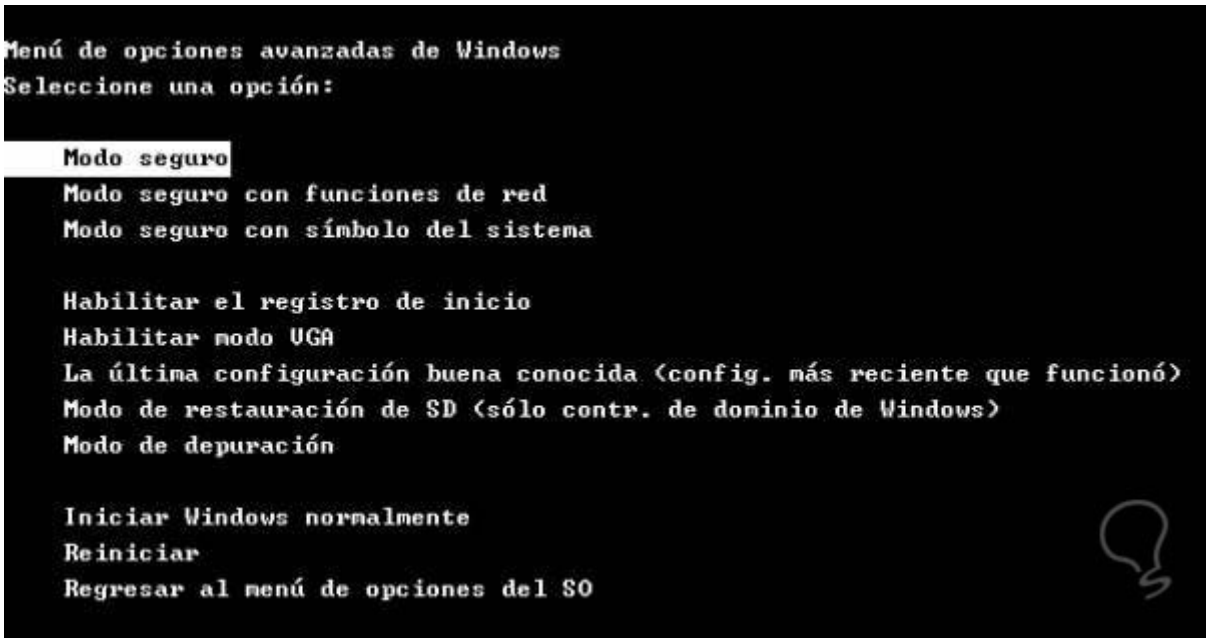
f) **Restaurar sistema**: Esta herramienta es muy útil cuando el equipo se nos vuelve inestable al instalar un nuevo programa ya que por nos permite devolver el sistema operativo a estados de

configuración anteriores respetando los archivos, de forma que no se pierda el trabajo realizado, ni siquiera el guardado desde el punto de restauración. La ruta para acceder a esta herramienta es Panel de Control – Recuperación – Abrir recuperar sistema, y así accedemos a un asistente sencillo que nos guiará en el proceso de restauración . Incluso al acabar la restauración nos ofrecerá la posibilidad de devolver el sistema operativo al estado anterior a la restauración. Al restaurar el sistema elegiremos un punto de restauración anterior a la aparición del problema a solucionar.
Esta aplicación está por defecto activa y por lo general está configurada de forma que se le un porcentaje de memoria adecuado a la misma que podríamos cambiar en Panel de control – Recuperación - Protección del sistema - Configurar. Si seguimos la ruta Panel de control - Recuperación - Configurar restaurar sistema – Protección del sistema – Crear podemos crear nuestros propios puntos de restauración aparte de los que ya realiza el sistema antes de cada operación que entienda como peligrosa (Instalar, Desinstalar, Actualizaciones).



g) **Modo a prueba de errores o modo seguro**:Windows nos permite cargar un “sistema operativo de emergencia” (normalmente en este modo se cargan los mínimos programas necesarios, y generalmente se deshabilitan muchos dispositivos no esenciales, con la excepción de los periféricos de entrada y salida básicos) para poder realizar reparaciones empleando herramientas propias del sistema o programas “Reparadores“ cuando el Sistema se ha venido abajo y ni siquiera no permite el acceso al mismo, o incluso con la intención de recuperar archivos antes de formatear el disco duro.

A este modo seguro se accede pulsando repetidamente alguna tecla o combinación de teclas (la tecla F8 es bastante habitual) antes de que se cargue el sistema operativo y nos aparecerá una serie de opciones (Modo Seguro , Modo seguro con funciones de red , Última configuración que ha funcionado ... etc). Ünicamente se carga el núcleo del programa por lo que notaremos que la pantalla se ve peor calidad y pixelada.



h) **Contraseñas**: Como regla de oro, debemos evitar dar nuestros datos personales en Internet, salvo en aquellas páginas en las que tengamos plena confianza. Por supuesto, esto incluye cualquier información personal, familiar, financiera o de costumbres. Absolutamente ningún banco nos va a pedir nunca nuestro número de cuenta, DNI o tarjeta por Internet ni por correo electrónico, por lo que NUNCA debemos facilitar estos datos si supuestamente nuestro banco nos los pide. Además, si las claves de acceso son ellos los que nos las generan y facilitan... ¿qué sentido tiene que luego nos las pidan vía E-Mail?.

No debemos guardar nuestras claves y contraseñas en el ordenador, y tampoco habilitar la opción de que algunos programas y páginas Web recuerden estas contraseñas. Si hacemos esto la utilidad de la contraseña se pierde completamente. Otro punto de gran importancia es el tipo de claves que solemos utilizar. Una clave, para ser medianamente segura tiene que constar al menos de 8 dígitos alfanuméricos, a ser posible mezclados números y letras, y si el programa nos lo permite, mezclar mayúsculas y minúsculas, y por supuesto sin tener ninguna relación con nosotros. La mayoría de los programas para romper claves se basan en una serie da algoritmos preestablecidos sobre las combinaciones más habituales a estudiar y mediante el método de la fuerza bruta. Es decir, que a partir de un dato conocido (y a algunos se les pueden introducir más de uno), empieza a generar una serie de combinaciones y a ejecutar combinaciones que guarda en una base de datos. Estas combinaciones están basadas en los criterios más usuales utilizados en las claves. Hay que tener también cuidado con las habituales preguntas para recordar la contraseña. Cualquier persona que nos conozca mínimamente puede acceder a estos datos en cuestión de minutos.

i) **Encriptación**: El cifrado de mensajes es sin duda uno de los sistemas más antiguos para proteger las comunicaciones. Diferentes sistemas de codificación, han ido evolucionando a lo largo de la historia, pero ha sido con la aplicación de máquinas y ordenadores a la criptografía cuando los algoritmos han conseguido verdadera complejidad.

Cifrado simétrico: Utiliza la misma clave para cifrar y descifrar. La clave es compartida por el emisor y por el receptor del mensaje, usándola el primero para codificar el mensaje y el segundo para descodificarlo.

Cifrado asimétrico: Utiliza dos claves distintas, una para cifrar y otra para descifrar. La clave para cifrar es compartida y pública, la clave para descifrar es secreta y privada. El emisor utiliza la clave

pública del receptor para cifrar el mensaje y, al recibirlo, el receptor utiliza su propia clave privada para descifrarlo. Este tipo de criptografía es también llamada de clave pública.

El programa gratuito PixelCryptor nos permite encriptar la información utilizando una imagen como contraseña de una forma muy sencilla.

j) **Navegación segura (https)**: El protocolo de comunicación más utilizado antiguamente en internet era el http:// pero tenía un grave problema no era seguro porque la información no está encriptada (cifrada). Ante esta situación se desarrolló el protocolo https:// que es el protocolo de comunicación que conecta nuestro navegador y el servidor de la página web a la que queremos acceder de forma segura gracias a la encriptación SSL ,que mediante un sistema de certificados digitales facilita el proceso de enlace y establece comunicaciones cifradas entre el navegador y un servidor web.(la información se transmite en un idioma que sólo conocen el navegador y el servidor por lo que aunque alguien capte la información no podrá entenderla). El protocolo SSL (Capa de puertos seguros) ha sido mejorado por el **TLS** (Seguridad de la capa de transporte) que es el que se utiliza hoy en día ya que utiliza algoritmos criptográficos más seguros.

No debemos realizar ninguna operación bancaria ni de pago en internet con páginas que no tengan este protocolo.

k) **Seguridade de nuestra red Wi-Fi**: En nuestras casas es muy habitual trabajar con redes Wi-Fi, para estar seguro de que nadie externo la está utilizando existe una aplicación para móvil que se denomina Fing que nos proporciona todos los datos de los equipos que están conectados en ese momento con nuestra red: nombre, IP y dirección MAC de la tarjeta de red.

Como características xerais das redes Wi-Fi podemos sinalar:

- Todas as redes sen fíos perden a seguridade que ofrecen as LAN cableadas, dado que é posible acceder a elas sen necesidade de acceso ao entorno físico.

- Calquera equipo que se conecte á rede sen fíos terá acceso ao resto da rede. É imprescindible protexer os equipos para que, se se da a intrusión, se manteña a máxima seguridade posible, pero tamén debemos evitar que sistemas non autorizados rompan a seguridade sen fíos e se podan conectar.

- Podemos establecer unha serie de consellos básicos de seguridade para a nosa rede:

    - Non deixes a rede sen fíos aberta, sen protección (sen contrasinal), posto que calquera podería acceder aos nosos datos privados e ademais reduciríase o ancho de banda, posto que teriamos que repartilo entre os equipos que se conecten.

    - Cambia a configuración por defecto do router. Aínda que agora a maioría dos routers levan activada unha encriptación básica, cun contrasinal que vén de fábrica e que está indicada no manual ou nunha pegatina pegada ao propio router, este contrasinal é facilmente descifrable. Para acceder á configuración do router e cambiala, debemos escribir a súa dirección no navegador, (debería vir indicado no manual do router, por exemplo 192.168.0.1). Dende aquí poderás cambiar calquera aspecto que estimes, empezando polo **nome da propia rede (SSID) e o contrasinal** necesario para unirse á rede e que debe ser diferente do contrasinal para acceder á configuración do router.

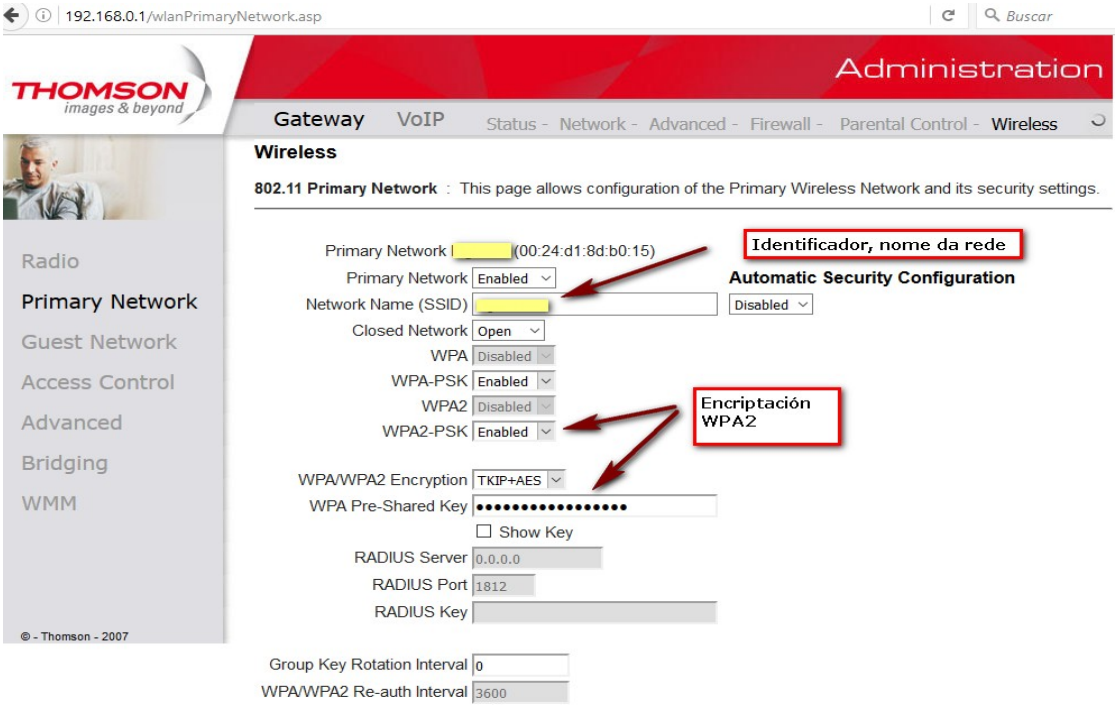
    - Debemos utilizar algún tipo de encriptación na nosa rede, onde a información debe viaxar encriptada cun algoritmo de complexa desencriptación, cunha lonxitude de contrasinal de encriptación o máis longa posible, se pode ser 512 bits, non utilicemos 128.

    Os routers sen fíos poden utilizar diferentes tipos de encriptación, por exemplo:

        - WEP. É o tipo de encriptación que incorporan por defecto, algoritmo non moi fiable, de fácil desencriptado.
        - WPA. É un protocolo máis robusto que o anterior. Non é indescifrable, o desencriptado pódese realizar utilizando dicionarios e forza bruta, pero se mantemos unha boa política de contrasinais, é moi fiable.
        - **WPA2**. O algoritmo máis completo, é un algoritmo complexo e de difícil desencriptación.
        - **WPA3.** O algoritmo WPA2 xa non é totalmente seguro e é substituido por o WPA3 que ten unha clave de cifrado máis difícil de romper.

Na seguinte ventá introduciríamos o nome de usuario e contrasinal para configurar a rede:

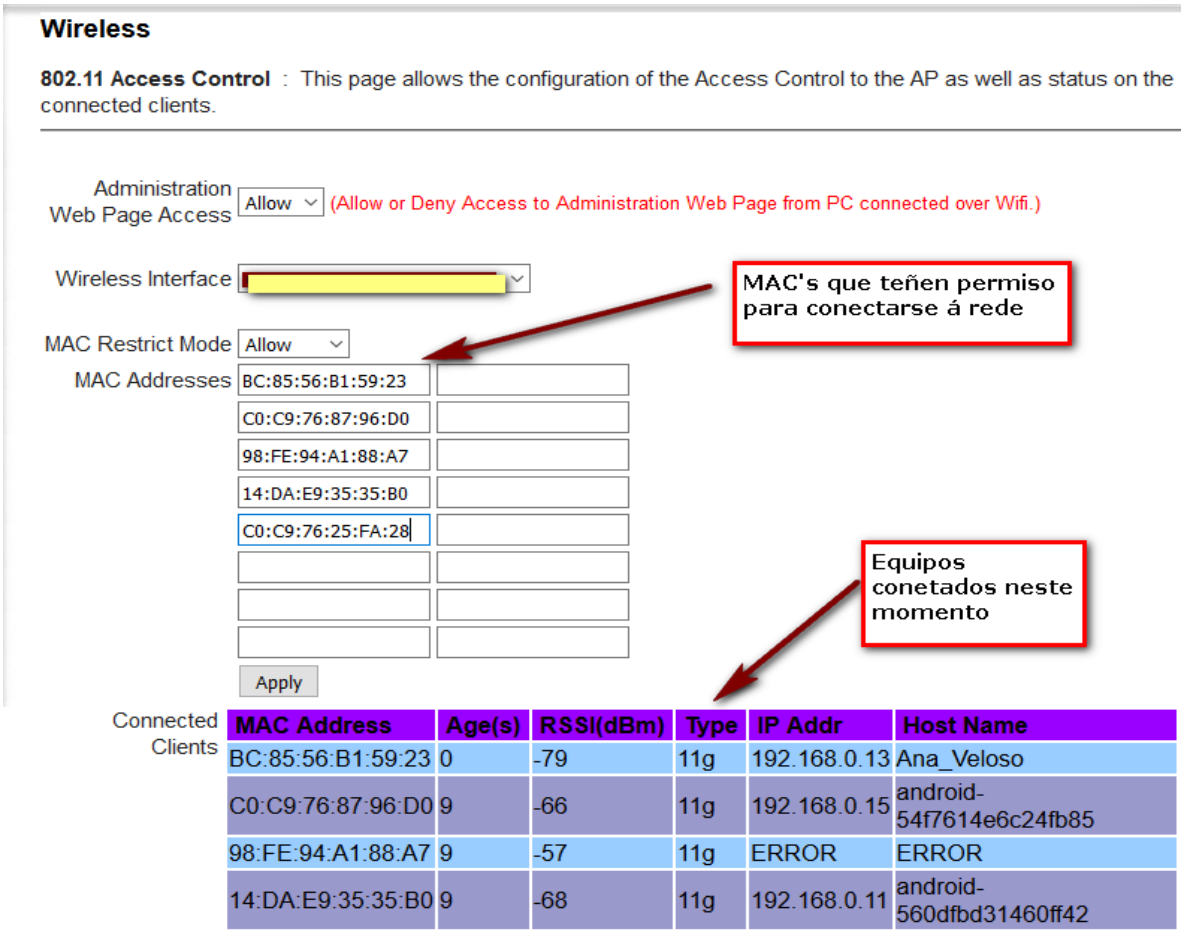
E nesta ventá establecemos a encriptación WPA2



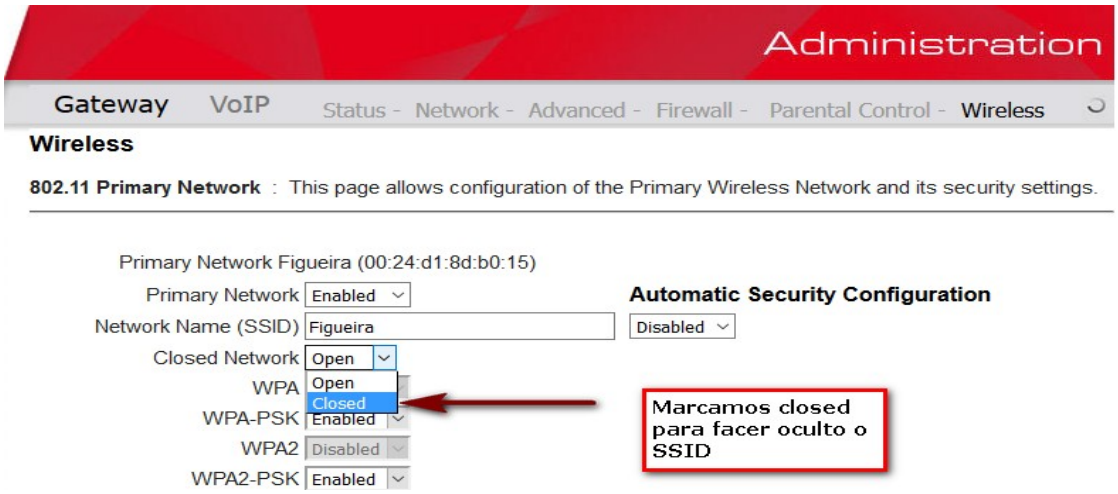
Podemos proporcionar aínda máis seguridade adicional á nosa rede sen fíos, para o cal:

- Creamos unha lista coas direccións MAC que desexemos se conecten á rede. Cada dispositivo con tarxeta de rede sen fíos, xa sexa móvil, tablet u ordenador, ten unha dirección única que o identifica, a dirección MAC. Con esa información, podemos crear unha lista de dispositivos autorizados na nosa rede, para que ningún outro dispositivo se poda conectar sen que lle deamos de alta a súa dirección na lista. De todos os xeitos, esta medida tampouco é infalible, xa que un usuario avanzado con malas intencións pode simular que a MAC do seu ordenador é unha das MAC autorizadas.
- Comprobar que dispositivos están conectados á nosa rede. Desta forma, podemos saber se temos un intruso, e actuar en consecuencia, cambiando inmediatamente o contrasinal e o SSID (nome) da nosa rede.

- Actualizar o firmware. Recordemos que o firmware é o software que controla os dispositivos. Habitualmente, os fabricantes proporcionan actualizacións para subsanar errores de seguridade detectados, para mellorar o rendimento, ...

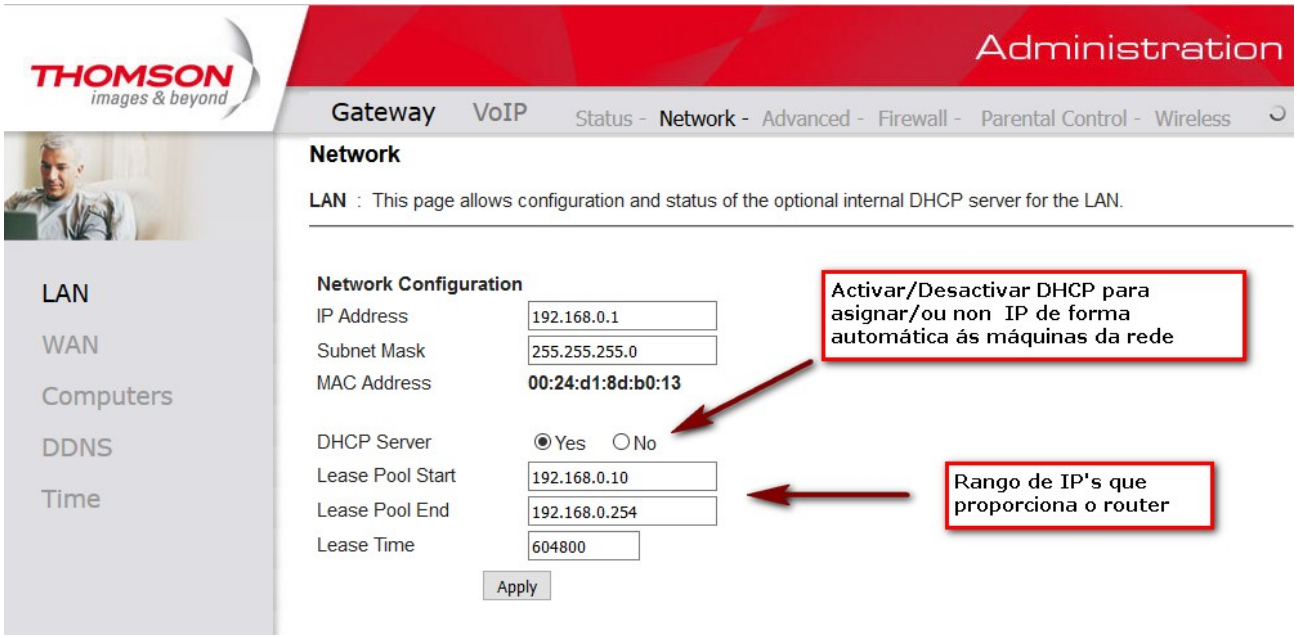


- **Ocultamos a nosa rede**, indicando que o SSID non sexa visible. Aínda que existen ferramentas que poden revelar este nome con facilidade, sempre complica as cousas un pouco. Ademais, para moitos, se non se ve, non existe, polo que a rede pasará desapercibida para moitos posibles agresores.



- **Limitar o número de conexións á rede**, para que non haxa máis das que necesites, de xeito que cando chegue ao máximo establecido, non admitirá novas conexións. Se nalgún momento necesitamos aumentar o número de dispositivos que se poden conectar simultaneamente, podemos ampliala temporalmente.
- Configurar o router para que **só se poda acceder e configurar dende unha conexión LAN**, e non a través da rede WiFi.

- Tamén é unha boa opción **desactivar o DHCP** e asociar direccións MAC a IPs de maneira estática no router.



l) **Navegación en modo incógnito**, este tipo de navegación mellora a privacidade, xa que o navegador non gardará o historial de navegación, as cookies e datos de sitios ou a información introducida en formularios, aínda así é probable que o noso proveedor de servizos en internet poida ver a nosa navegación.

Respeto de la propiedad intelectual

Internet puede proporcionarnos mucha información y servicios de interés. También podemos encontrar en la Red software de todo tipo que nos pueda interesar conseguir. Es muy importante conocer que el software, al igual que otras creaciones como los libros, canciones, cuadros ,… están protegidos por la ley de propiedad intelectual.

Los derechos de autor son un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley reconoce a los autores por la creación de una obra publicada o inédita. La propiedad intelectual agrupa todos los derechos del autor sobre la disposición y explotación de su creación.

Cuando accedemos a una página web para descargarnos alguna aplicación es muy importante que conozcamos con qué tipo de licencia se corresponde el software que queremos descargar. No todas las descargas son ilegales o atentan contra la propiedad intelectual.

Debemos distinguir entre:

Software comercial: Software de una empresa que se comercializar con ánimo de lucro. Ejemplo: windows 10 o Microsoft Office. Todo el software comercial es propietario. Utiliza **licencias copyright** en la que están todos los derechos reservados.

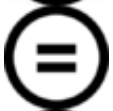
Software libre: Se puede usar, copiar, modificar y redistribuir libremente. Su código fuente está disponible, lo que se conoce como código abierto. Ejemplo: Libre Office, GIMP, Audacity. Utiliza **licencias copyleft** en vez de copyright, que lo que hace es justo lo contrario otorga derechos: libre distribución, permite la modificación,… Un ejemplo de licencia copyleft es la licencia GNU/linux del software del sistema operativo de vuestros ordenadores de clase que asegura que las copias y derivados del mismo estén bajo la misma licencia.

Freeware: Es software gratuito pero no libre. Ejemplo: Adobe acrobat reader, Adobe flash player. Son gratis aunque tengan propietario.

Copyright - Copyleft 

Con la aparición de las nuevas tecnologías aparecieron muchos problemas con los derechos de autor, para solucionarlo surgieron las **licencias creative commons** con las que el creador de una obra puede decidir bajo que condiciones se puede utilizar sus imágenes, libros, música, software.

Estas son las licencias creative commons:

 **Reconocimiento (Attribution BY)**	Debe reconocerse la autoría de la obra de manera adecuada (en un lugar visible). Debemos mencionar el nombre del autor si utilizamos su trabajo.
 **No Comercial (NonCommercial NC)**	No se permite la utilización de la obra para fines comerciales.
 **Sin obras derivadas (NoDerivative Works – ND)**	No se permite la distribución de obras derivadas basadas en ella, por lo que no podemos transformar la obra para crear una derivada.
 **Compartir Igual (ShareAlike – SA)**	Si se crea una obra derivada, debe distribuirse bajo la misma licencia que la obra original.

LICENCIA	PERMITE	SIEMPRE QUE
Reconocimiento (BY)	Compartir (copiar y redistribuir) y adaptar (remezclar, transformar y construir a partir del material), incluso para fines comerciales.	■ Se reconozca la autoría de la obra original de forma adecuada.
Reconocimiento - Compartir Igual (BY-SA)	Compartir (copiar y redistribuir) y adaptar (remezclar, transformar y construir a partir del material), incluso para fines comerciales.	■ Se reconozca la autoría de la obra original de forma adecuada. ■ Se licencie la nueva creación (en su caso) bajo condiciones idénticas (BY-SA)
Reconocimiento - Sin Obra Derivada (BY-ND)	Compartir (copiar y redistribuir) el material, incluso para fines comerciales.	■ Se reconozca la autoría de la obra original de forma adecuada. ■ No se distribuyan modificaciones de la obra original.
Reconocimiento - No Comercial (BY-NC)	Compartir (copiar y redistribuir) y adaptar (remezclar, transformar y construir a partir del material).	■ Se reconozca la autoría de la obra original de forma adecuada. ■ No se utilice con propósitos comerciales.
Reconocimiento - No Comercial - Compartir Igual (BY-NC-SA)	Compartir (copiar y redistribuir) y adaptar (remezclar, transformar y construir a partir del material).	■ Se reconozca la autoría de la obra original de forma adecuada. ■ No se utilice con propósitos comerciales. ■ Se licencie la nueva creación (en su caso) bajo condiciones idénticas (BY-NC-SA)
Reconocimiento - No Comercial - Sin Obra Derivada (BY-NC-ND)	Compartir (copiar y redistribuir) el material.	■ Reconozca la autoría de la obra original de forma adecuada. ■ No se utilice con propósitos comerciales. ■ No se distribuyan modificaciones de la obra original.

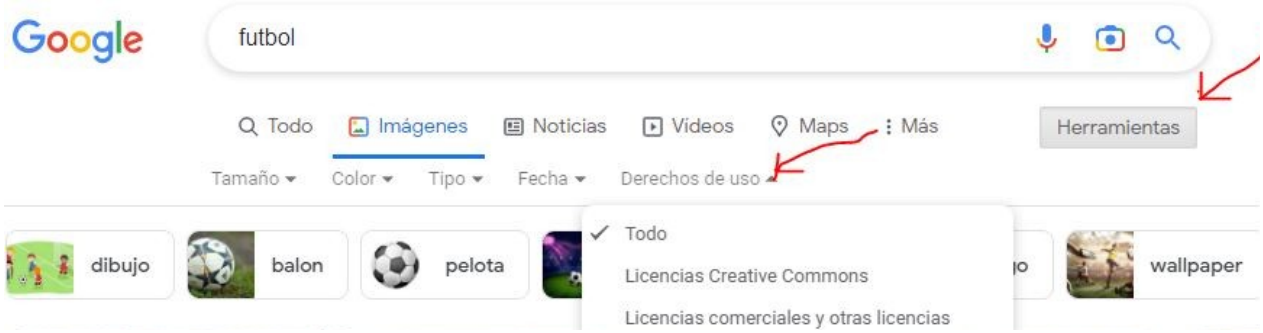
FUENTE: https://creativecommons.org/

cedec CENTRO NACIONAL DE DESARROLLO CURRICULAR EN SISTEMAS NO PROPIETARIOS

También existe la **CC-0** en la que el autor ha renunciado a todos sus derechos.

Fíjaros en la búsqueda de google que tipo de licencia tienen las fotos que descargais. Para esto pincha en herramientas y en Derechos de uso. Si escogéis Licencias comerciales pinchando en la imagen podréis ver sus derechos de autor.

En la siguiente página tenéis enlaces a páginas que proporcionan material libre de todo tipo (imágenes, sonidos, vídeos,…) : https://cedec.intef.es/bancos-gratuitos-de-imagenes-videos-y-sonidos/
Hay muchas páginas web que tienen imágenes libres para descargar: procomún, freepng, freeimages.
Entra en freepng.es donde se pueden descargar fotos e imágenes y comprueba la licencia de las mismas.



A veces las licencias vienen especifícadas simplemente como **permiso de uso personal** o **permiso de uso comercial**. Permiso de uso personal implicaría que podemos usar por ejemplo una imagen pero sólo para proyectos personales y nunca para ganar dinero. En cambio permiso de uso comercial si que nos permitiría ganar dinero con esa obra, por ejemplo si descargamos un dibujo con esta licencia y hacemos unas camisetas con el mismo, sería legal poder venderlas.

Firma digital

Firma electrónica simple

La firma electrónica simple firma es fácil y rápida ya que no se trata de un trazo como tal, sino que consiste en marcar una casilla o introducir un código PIN.

Esta es muy rápida de configurar, sin embargo, la validez legal en estos casos no está asegurada ya que no permite identificar al usuario de forma inequívoca. El usuario solo tiene que hacer clic en el botón de «Aceptar términos y condiciones» para mostrar su conformidad con el documento.

Su caso de uso más recomendado es para la firma de documentos con poco riesgo jurídico, como las condiciones generales de una web o para validar los días de vacaciones de un trabajador.

Firma electrónica avanzada

La firma electrónica avanzada tiene un nivel de seguridad superior al de la firma simple: las dos primeras condiciones definidas por el Reglamento europeo eIDAS aseguran que el firmante sólo puede haber sido aquel a quien se solicitó la firma, mientras que las dos últimas limitan extraordinariamente el riesgo de suplantación de identidad.

Para asegurar que la firma sólo puede asociarse a un único firmante, en el momento de la firma recopilamos un gran volumen de información y utilizamos un sellado de tiempo. El sellado de tiempo es un método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces.

1.Para identificar al firmante, se geolocaliza con exactitud el lugar en el que se ha realizado la firma, se registra las direcciones de origen y destino de la solicitud y la hora de la firma, y captura datos biométricos del grafo a partir de la presión ejercida en el dispositivo de firma (en aquellos dispositivos que lo permite). De este modo, se puede poner esta información a disposición de un grafólogo en caso de disputa para que pueda realizar su análisis de firmas.

2.Por último, se impide cualquier cambio ulterior en la firma y, por extensión, garantiza al solicitante y firmante que la firma obtenida no se puede modificar tras su realización. Para ello se cifra la documentación generada conforme a unos estándares de encriptación que garantizan su integridad al 100%.

La firma electrónica avanzada asegura la verificación de la identidad e integridad de los datos firmados. Además es una evidencia jurídica admisible como prueba en un juicio.

Firma electrónica cualificada

la firma electrónica cualificada es el método más complejo y seguro para acreditar digitalmente la identidad de un sujeto y que este pueda aceptar el contenido de un documento de forma irrevocable.

También llamada QES por sus siglas en inglés (Qualified Electronic Signature), esta firma electrónica reconocida o cualificada es la única firma digital respaldada por un certificado cualificado que permite identificar al firmante de forma fiable y que, además, protege los documentos firmados ante cualquier manipulación o falsificación de forma tan segura que permite a la firma electrónica cualificada tener la misma validez legal que la manuscrita.

Para ser así, la firma electrónica cualificada debe ser realizada con el respaldo de la emisión de un certificado cualificado de firma electrónica previo que identifique al firmante. Este certificado consiste en un documento electrónico que liga los datos del firmante y la validación de la firma a la

identidad inequívoca del sujeto. Dicho certificado únicamente puede haber sido expedido por una **autoridad de certificación cualificada**. (En España las principales autoridades de certificación para poder obtener un certificado digital son el DNI electrónico y la fábrica nacional de moneda y timbre)

Gracias a este certificado cualificado, la firma electrónica cualificada no necesitaría de ningún tipo de prueba pericial adicional ante un tribunal en caso de conflicto, ya que se considera una evidencia totalmente válida ante la ley y con el mayor nivel de legitimidad, originalidad e inviolabilidad exigible.

La firma electrónica cualificada comparte la mayoría de las características de la firma electrónica avanzada, tales como estar vinculada al firmante de forma única e intransferible o estar ligada al documento a firmar de forma inalterable, con la salvedad de que la avanzada no cuenta con el respaldo del certificado cualificado de firma electrónica, lo cual la pone por debajo de la cualificada ante la ley.

En la siguiente tabla tenemos un resumen de las tres opciones:

TIPO DE FIRMA ELECTRÓNICA	NIVEL DE SEGURIDAD	CARACTERÍSTICAS	DOCUMENTOS QUE SE PUEDEN FIRMAR
Simple	Bajo	No identifica de manera inequívoca al firmante	Documentos sin riesgos legales / financieros
Avanzada	Alto	Identifica de manera inequívoca al firmante y evita la modificación del documento firmado a través de técnicas como el sellado de tiempo o la firma biométrica	Todo tipo de documentos laborales y contratos
Cualificada	Alto	Identifica de manera inequívoca al firmante y evita la modificación del documento firmado a través de un Certificado Digital emitido por un Prestador de Servicios de Confianza acreditado	Trámites con las Administraciones Públicas

Para elegir qué tipo de firma electrónica necesitas debes tener en cuenta qué necesitas firmar y qué nivel de seguridad requieres. Si simplemente necesitas que el firmante acepte las condiciones legales de tu web puedes usar la firma electrónica simple pero si necesitas validar la identidad del firmante y evitar la posterior modificación del documento tienes que usar la firma electrónica avanzada o la firma electrónica cualificada.

Entra en este enlace: ¿Cómo obtener tu certificado digital de la FNMT)?

Mirad estos vídeos: ¿Cómo firmar un pdf con firma digital?

¿Cómo activar el DNI electrónico?

¿Cómo hacer una firma digital con el certificado del DNIe?