Sellos eco y medioambientales para dispositivos

Energy Star (EE.UU) (Sólo para productos electrónicos)

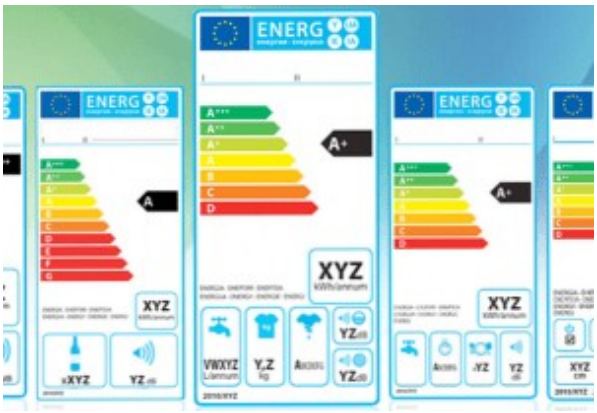
Los productos con esta etiqueta cumplen con los parámetros de eficiencia energética marcados por la Agencia de Protección Ambiental de los Estados Unidos (EPA, por sus siglas en inglés). Fue creada en 1992 para fomentar **los aparatos electrónicos** con una alta eficiencia energética, lo cual contribuye a emitir menos cantidad de CO_2 a la atmósfera y por tanto ser más respetuosos con el medio ambiente.

Eco Rating (Indicador para telefonía móvil)

La etiqueta Eco Rating muestra de una manera sencilla y clara el impacto medioambiental de los teléfonos móbiles. Incluye una puntación en una escala del 1 al 100 que evalúa cómo de sostenible es el móvil. Cuanto mayor es la puntuación más respetuoso es el teléfono con el planeta.

Etiqueta energética de la UE (Europa) (Para electrodomésticos)

El enfoque de este certificado es el ahorro energético. Esta etiqueta indica la cantidad de energía que consume un **electrodoméstico**. Para ello, se utiliza un rango de la A+++ a la D, siendo la primera la menos contaminante, y la D la más contaminante. Para recibir una calificación de A+++, una nevera, por ejemplo, debe consumir menos del 22% de la energía que un producto de referencia comparable usa anualmente. Este certificado nos resulta muy útil, no solo para saber que hacemos una compra ecológica, sino porque al comprar los productos menos contaminantes, veremos muy reducida nuestra factura de la luz.



EPEAT (Global)

EPEAT es una herramienta de clasificación ambiental, cuyas siglas hacen referencia a «Evaluación Ambiental de Productos Electrónicos». A diferencia de las anteriores mencionadas, EPEAT es un sistema estándar utilizado en todo el mundo, tanto por empresas globales y gobiernos como por consumidores que quieren comprar electrónica más sostenible. Los productos EPEAT registrados garantizan un nivel más bajo de cadmio, plomo, mercurio y otros tóxicos, para proteger no solo el Planeta, sino también nuestra salud.

Etiqueta ecológica de la UE (Europa)
La Comunidad Europea introdujo esta etiqueta en 1992, para ayudar a los consumidores a identificar productos y servicios con un impacto ambiental reducido durante todo su ciclo de vida. Esta etiqueta no solo cubre productos electrónicos, sino una amplia gama de artículos como bombillas, detergentes, etc.

TCO Certified (Global)

Al igual que EPEAT, TCO también es una certificación internacional del ciclo de vida de productos IT. Pero TCO va más allá, y también incorporan fabricación, ergonomía, ambiente de trabajo, salud y seguridad socialmente responsables.

Protocolo de 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 p**rotocolo 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.

Mira el siguiente vídeo sobre SSL, TLS y https://

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. El cifrado puede ser de dos tipos:

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.

Mira este vídeo sobre cifrado simétrico y asimétrico.

Medidas de seguridad

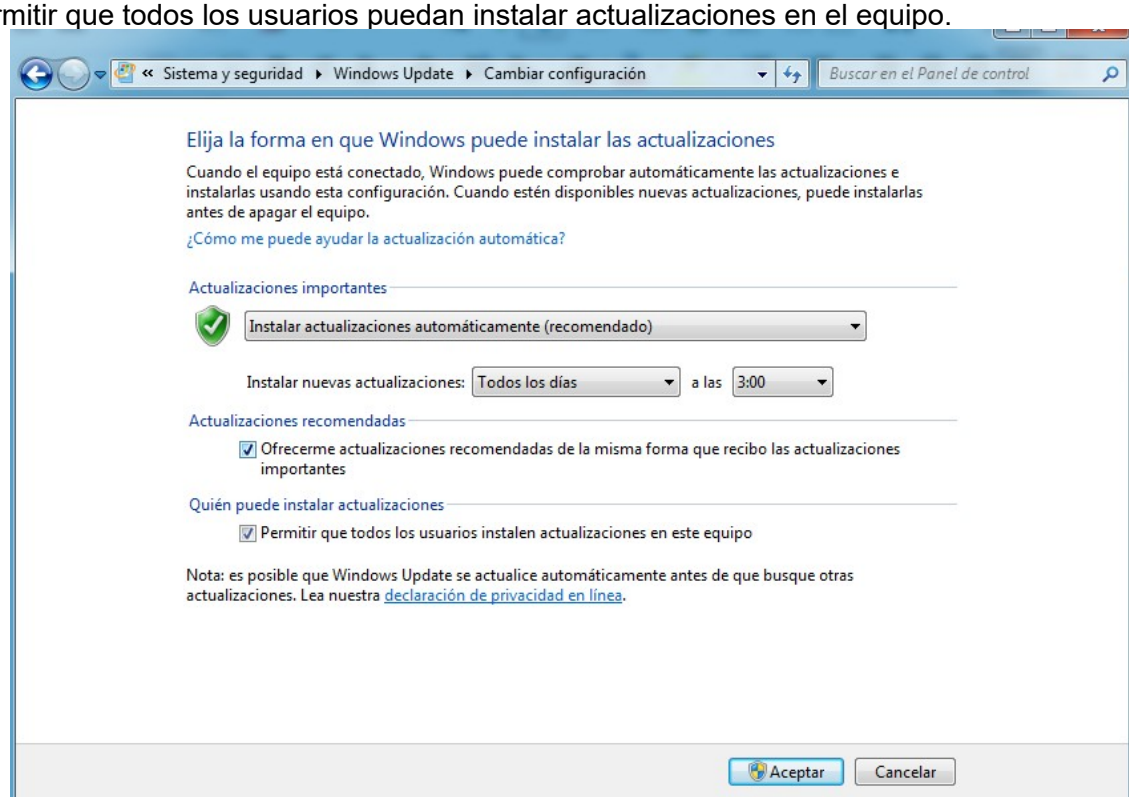
Para proteger nuestros sistemas informáticos tenemos dos tipos de medidas, de seguridad activa y de **seguridad pasiva**. Las medidas de **seguridad activa** buscan evitar daños e intrusiones en los equipos, en su software y en la información que contienen. Un ejemplo sería un antivirus. Por otro lado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

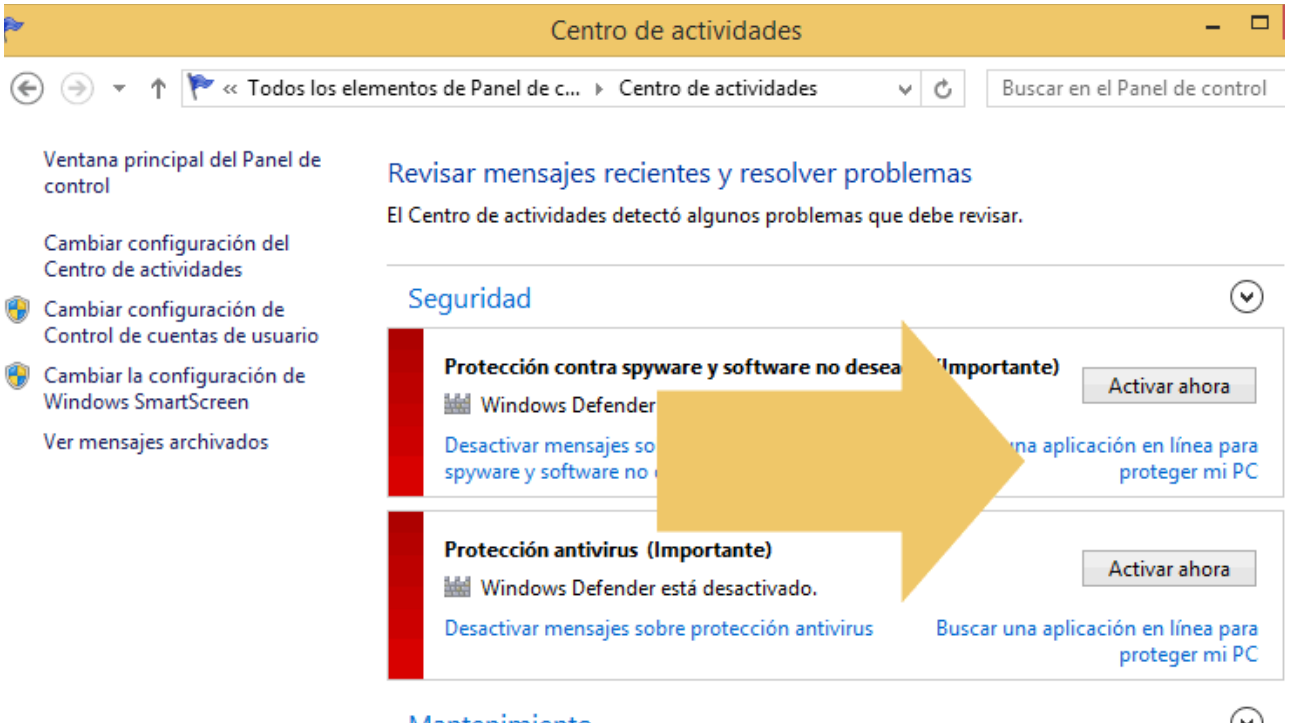
1. **Tener el sistema operativo actualizado y programadas las actualizaciones automáticas**

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.



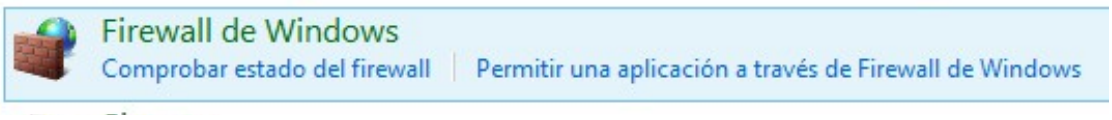
Entre los antivirus gratuitos destacan el AVG (http://www.avg.com/es-es/homepage) y el AVAST (https://www.avast.com/es-es/index)

3. **Tener el firewall (cortafuegos) activado**

Puede ser un dispositivo físico (hardware) o un programa (software) 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. 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.



Mira el vídeo: ¿Qué es un firewall o cortafuegos?

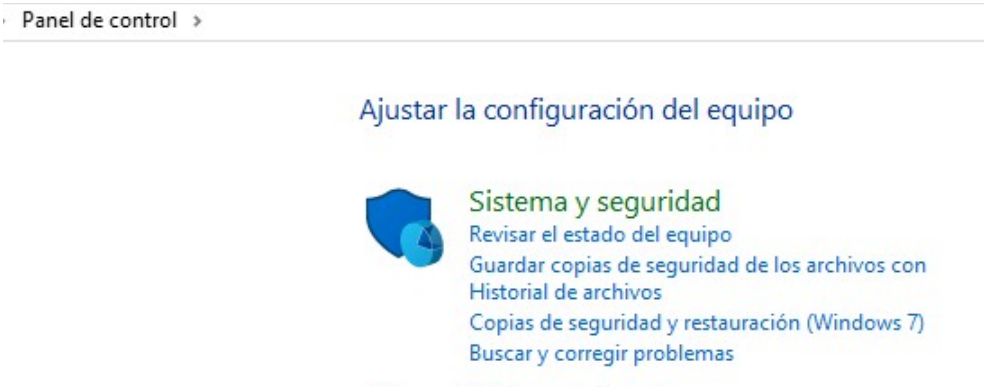
Estas tres primeras medidas son de seguridad activa, la siguiente, la realización de copias de seguridad es una medida de seguridad pasiva.

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.

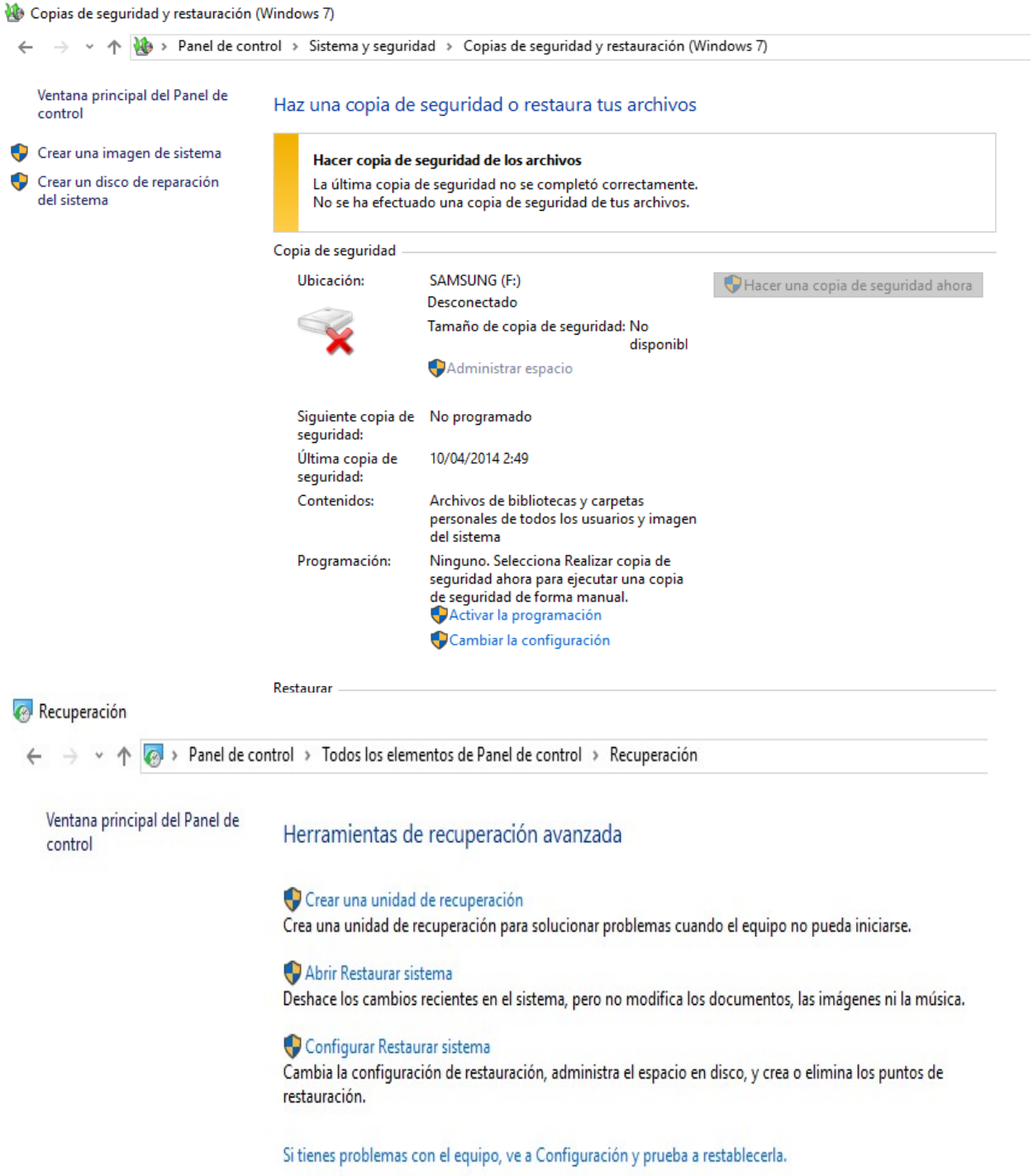
La copia de seguridad puede hacerse a muchos niveles dependiendo de qué es lo que intentemos proteger, desde un solo archivo hasta una partición de disco duro, o incluso el disco duro completo incluyendo los diferentes S.O. que podamos tener en sus particiones, los drivers y el resto del contenido . 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.

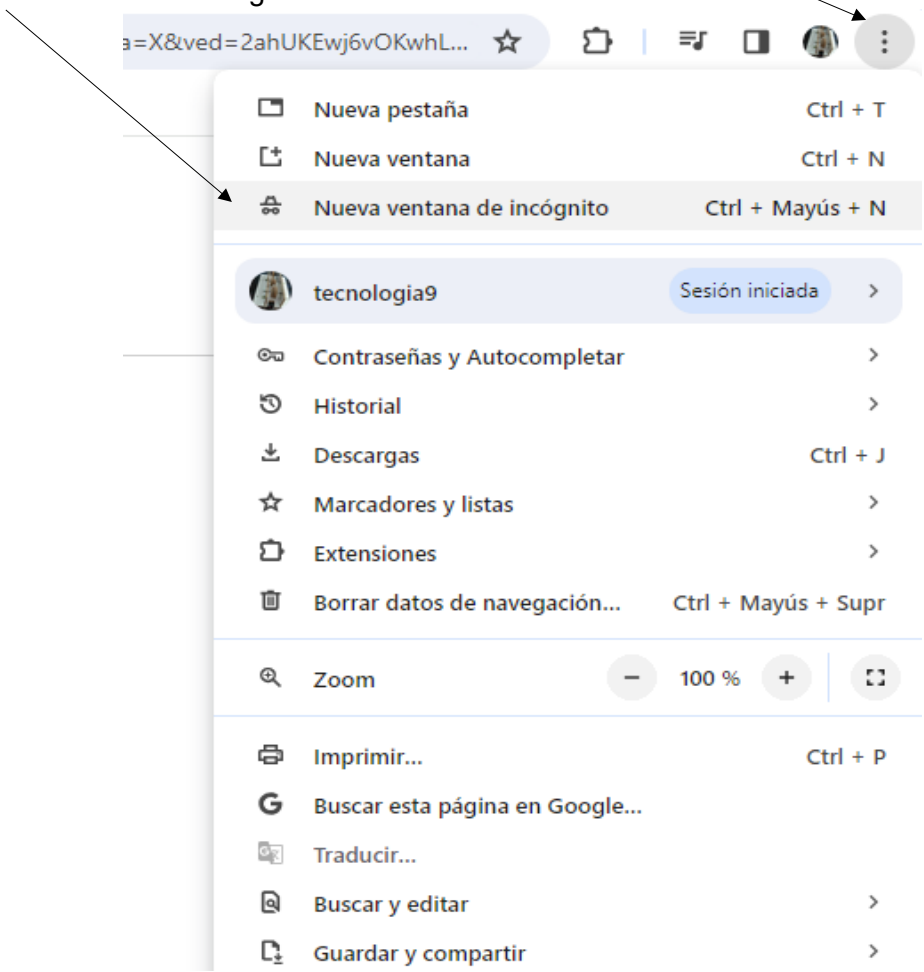
También nos permite hacer una imagen del sistema (en la que queda guardado absolutamente todo: archivos, programas y sistema operativo). Hoy en día muchos ordenadores traen una imagen del sistema en una partición del disco duro. En caso de colapso total de tal forma que no aparezca el menú de arranque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



Navegación en modo incógnito

Este tipo de navegación mejora la privacidad, ya que el navegador no gardará el historial de navegación, las cookies y datos de sitios o la información introducida en formularios. Los sitios web que visites, tu empresa o centro educativo y tu proveedor de servicios de internet si pueden seguir viendo tu actividad en la red.

Para acceder al modo incógnito en chrome pinchamos en la esquina superior derecha en los tres puntos y después en Nueva ventana de incógnito.



Si quieres saber lo que son las cookies pincha en: ¿Qué son las cookies en 1 minuto?

Seguridad de una red wifi

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 algúns aspectos 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.

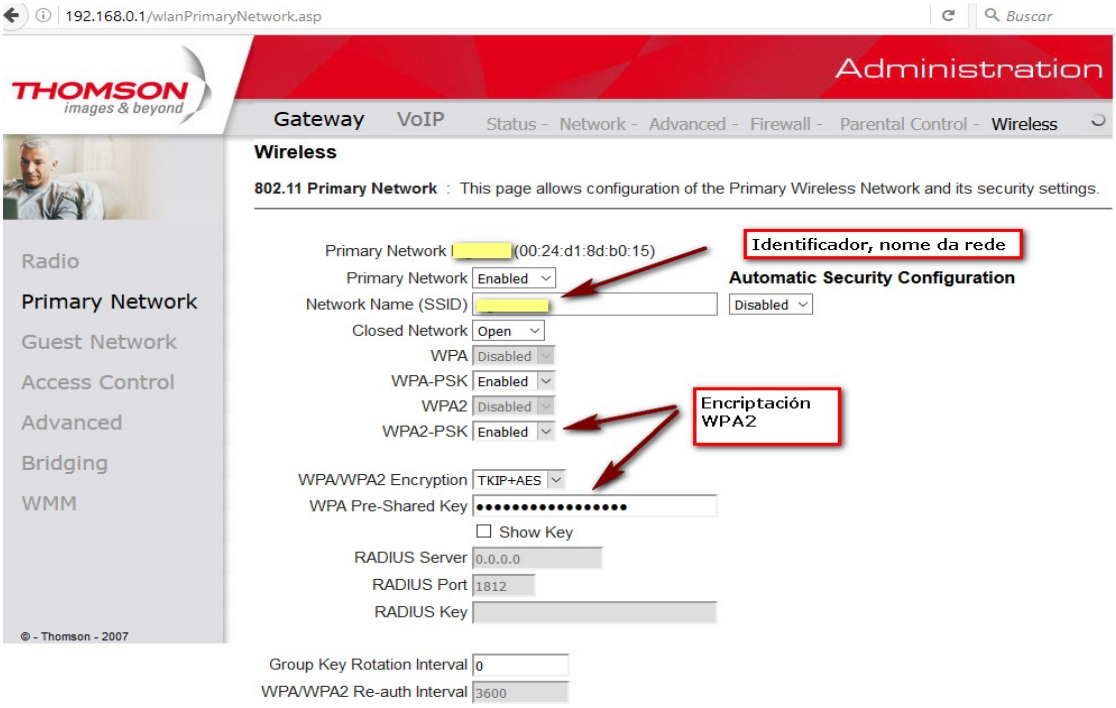
    - Debemos utilizar algún tipo de encriptación na nosa rede, onde a información debe viaxar encriptada cun algoritmo de complexa desencriptación, cunha lonxitude de contrasinal de encriptación o máis longa posible, se pode ser 512 bits, non utilicemos 128.

    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

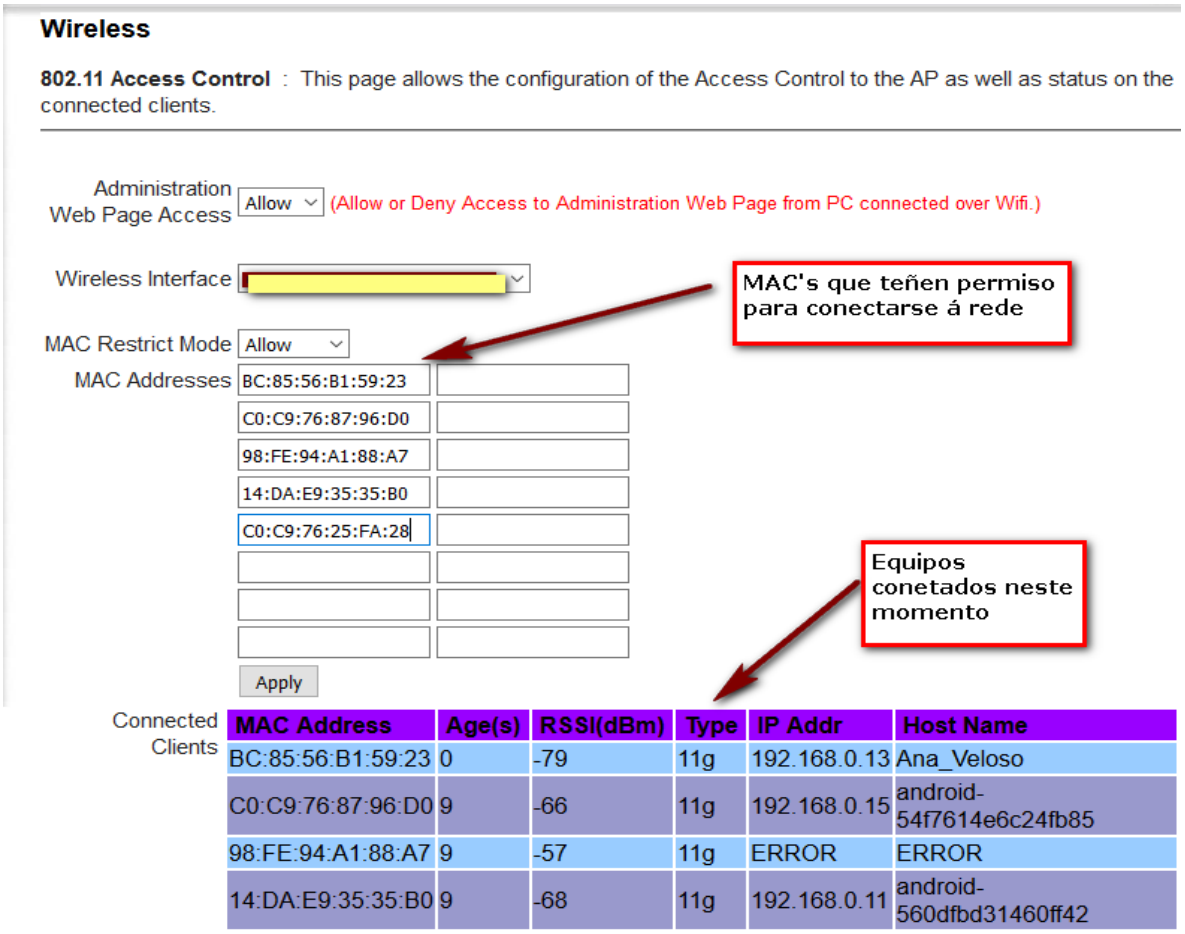


Podemos proporcionar aínda máis seguridade adicional á nosa rede sen fíos, para o cal:

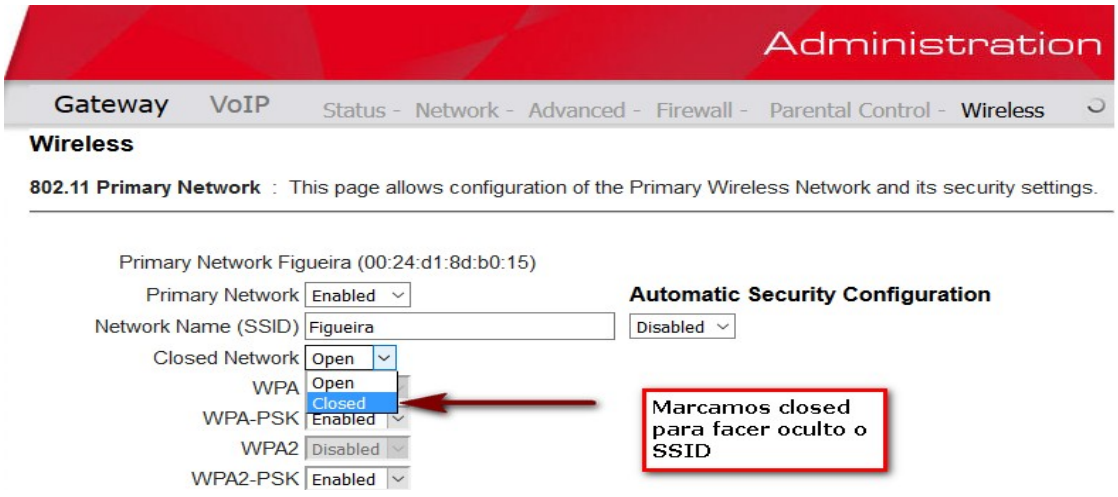
- Creamos unha lista coas direccións MAC que desexemos se conecten á rede. Cada dispositivo con tarxeta de rede sen fíos, xa sexa móvil, tablet u ordenador, ten unha dirección única que o identifica, a dirección MAC. Con esa información, podemos crear unha lista de dispositivos autorizados na nosa rede, 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.

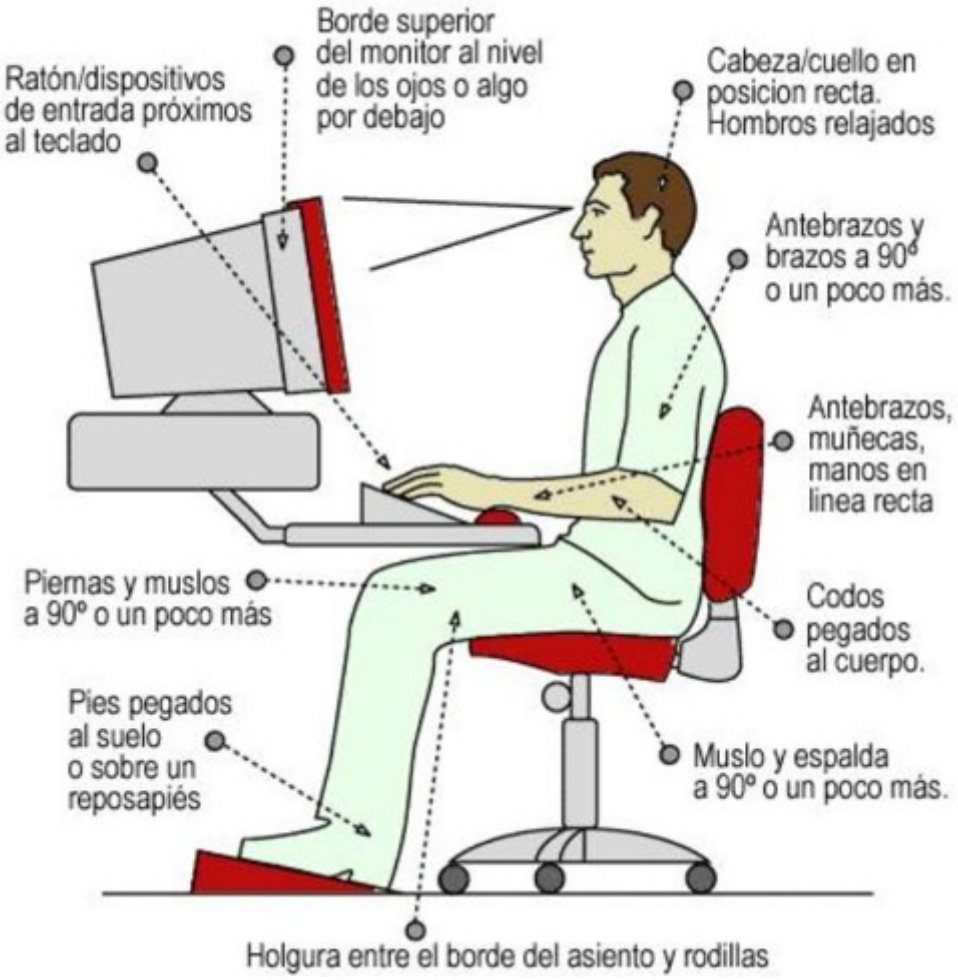
- Actualizar o firmware. Recordemos que o firmware é o software que controla os dispositivos. Habitualmente, os fabricantes proporcionan actualizacións para subsanar errores de seguridade detectados, para mellorar o rendimento, ...



- **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.



Ergonomía en el trabajo con el ordenador



Mira esta página que añade un poco más de información de otros aspectos: La ergonomía del informático.

Otras posibles preguntas:

- En un simulador de un móvil os piden que lo configuréis para que se ponga en modo reposo tras 15 segundos de inactividad.

- Para que sirve el modo oscuro? Se consigue un ahorro energético porque los píxeles oscuros están apagados y como recomiendan que la luz de los dispositivos se asemeje a la luz ambiental, el modo oscuro es más adecuado cuando es de noche o en ambientes de poca luz. En un móvil se activa Ajustes – Pantalla – Tema oscuro. En Google Chrome hacemos click en los tres puntos de la esquina superior derecha – Configuración – Aspecto – Modo Oscuro.

- ¿Cómo saber si mi navegador Google Chrome está actualizado? Hacemos click en los tres puntos de la esquina superior derecha – Ayuda – Información de Google Chrome o Acerca de Google Chrome.