10 CONSEJOS PARA PROTEGER TU NUEVO COMPUTADOR

¿Te has comprado un nuevo computador y acaba de llegarte? ¿Quieres saber cuál puede ser la mejor forma de mantenerlo seguro, y de proteger tus datos?

EN ESTE ARTÍCULO, TE EXPLICAMOS ALGUNOS PASOS PARA QUE PUEDAS CONFIGURARLO DE LA MEJOR MANERA CON EL OBJETIVO DE MANTENERLO SEGURO.

En la actualidad, no es extraño que tengamos en casa uno o más computadores. Basamos una parte de nuestra vida en estos dispositivos, así que es muy importante que sepamos cómo proteger los datos que guardamos en ellos.

Por ese motivo, te proporcionamos los siguientes consejos para ayudarte en esta importante tarea. ¡Síguelos y protégete!

¿QUÉ TE RECOMENDAMOS?

1. Mantén tu equipo actualizado con las últimas actualizaciones disponibles.
2. Protege tu cuenta de usuario con una contraseña robusta.
3. Deshabilita el inicio de sesión automático.
4. Configura el bloqueo del equipo cuando estás ausente o entra en reposo
5. Usa programas antivirus de confianza y mantenlo actualizado.
6. Desinstala las aplicaciones basura que vienen preinstaladas y aquellas que no vayas a utilizar.
7. Revisa las opciones de privacidad y configúralas según tus necesidades.
8. Deshabilita la conexión wifi y Bluetooth cuando no la uses.
9. Activa el *firewall*.
10. Habilita el cifrado de disco.

¿CÓMO PUEDES HACERLO?

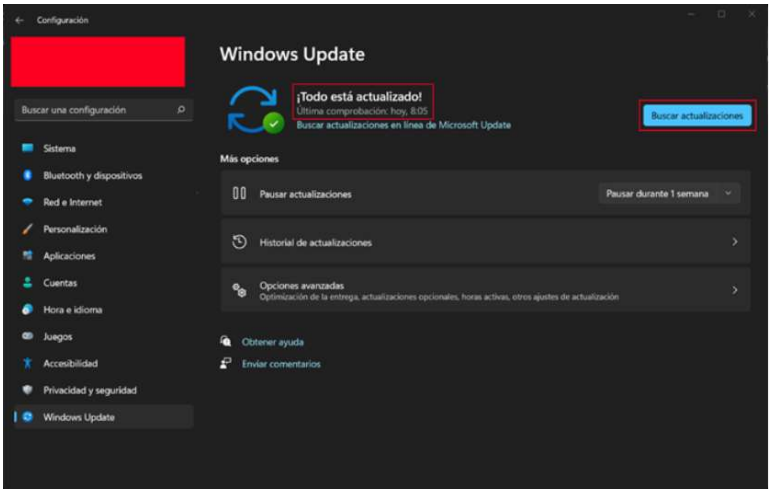
1. **Mantén tu equipo actualizado con las últimas actualizaciones disponibles.**

   Es muy importante mantener actualizado el sistema operativo, controladores y aplicaciones de nuestro computador, ya que las actualizaciones mejoran el rendimiento y corrigen vulnerabilidades.

En Windows

Abre la aplicación de '**Configuración**' desde el menú 'Inicio', ve a '**Windows *Update***' y pulsa en el botón '**Buscar actualizaciones**' para ver si hay nuevas actualizaciones disponibles.

En caso de no haber actualizaciones, aparecerá el mensaje '**¡Todo está actualizado!**'.



En caso de haber nuevas actualizaciones, aparecería como en la siguiente imagen, con el mensaje '**Actualizaciones disponibles para instalar**' y haríamos clic en '**Instalar ahora**'.

Una vez instaladas, te pedirá reiniciar el computador para aplicar las actualizaciones, podemos hacer clic en '**Reiniciar ahora**' para ello.

EN MAC

En el menú Apple (en la esquina superior izquierda de la pantalla), entra a '**Preferencias del sistema**' > '**Actualización de software**'. Si hay alguna actualización disponible, haz clic en '**Actualiza ahora**' para instalarla.

2. Protege tu cuenta de usuario con una contraseña robusta.

Para que una contraseña sea fuerte, debe cumplir:

- Tener una longitud mínima de 8 caracteres.
- Contener caracteres alfanuméricos (letras minúsculas, mayúsculas y números).
- Contener caracteres especiales ($, #, &, etc.).
- No tiene que contener datos personales, como fechas relevantes, nombres propios…

En Windows

Ve a '**Configuración**' > '**Cuentas**' > '**Opciones de inicio de sesión**'. En el apartado '**Contraseña**' podrás poner una o cambiarla, si ya lo habías hecho.

En Mac

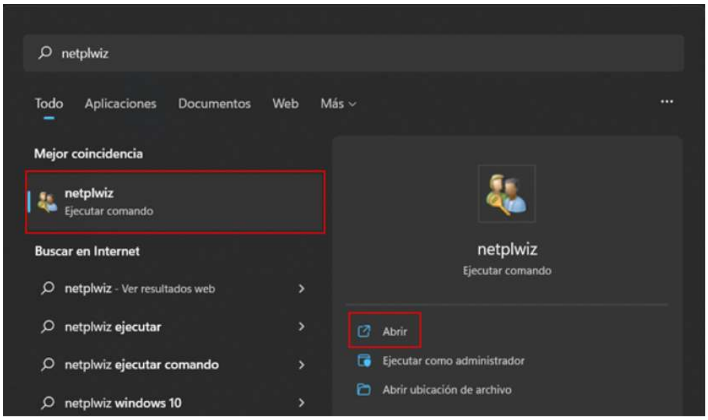
Ve a '**Preferencias del sistema** > '**Usuarios y grupos**'. Aquí selecciona tu usuario y haz clic en '**Cambiar contraseña**'.

3. Deshabilita el inicio de sesión automático.

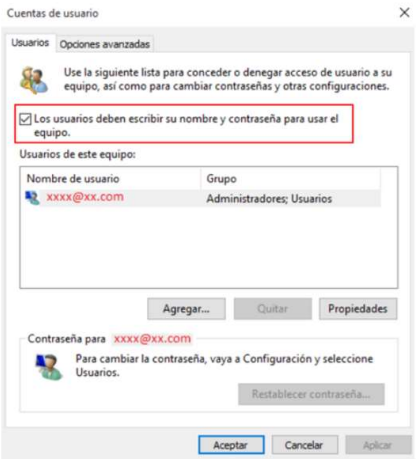
Si somos los únicos que usamos nuestro computador, es bastante cómodo, que queramos habilitar el inicio automático de sesión. Esta práctica es peligrosa porque cualquier persona que tenga acceso al equipo, podrá iniciar sesión en él y llegar así a nuestros datos. Por eso, lo mejor es comprobar si esta opción está desactivada.

En Windows

Para comprobarlo, abre el menú Inicio y en el campo de búsqueda escribe '**netplwiz**'. Haz clic sobre la aplicación que aparece en la siguiente imagen.



Una vez se abra la ventana, como en la siguiente imagen, asegúrate que la casilla '**Los usuarios deben escribir su nombre y contraseña para usar el equipo**' esté marcada, antes de cerrar la ventana y no olvides '**Aplicar los cambios**'.



En Mac

Ve a '**Preferencias del sistema**' > '**Usuarios y grupos**'. Haz clic en el icono del candado (en la parte inferior de la ventana) y escribe la contraseña de la cuenta. Haz clic en '**Opciones de inicio**', en la esquina inferior izquierda, y asegúrate de seleccionar la opción '**Desactivado**' en el menú desplegable '**Inicio de sesión automático**'.

4. Configura el bloqueo automático del equipo cuando estás ausente o entra en reposo.

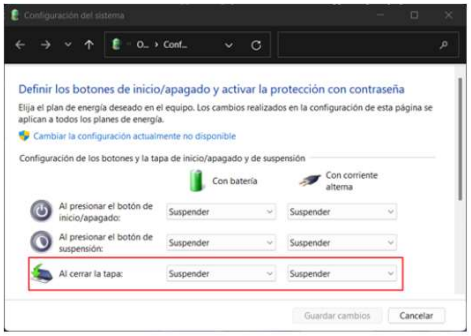
Cuando te levantes para descansar o no vayas a utilizar el computador en un rato, es importante bloquearlo, para que otras personas no tengan acceso a él.

Los siguientes casos, son ejemplos de cuándo se bloquea el equipo:

- Dejar de teclear y usar el ratón por un tiempo definido según los ajustes.
- Tener un computador portátil y cerrar la tapa.
- Se bloquea manualmente.

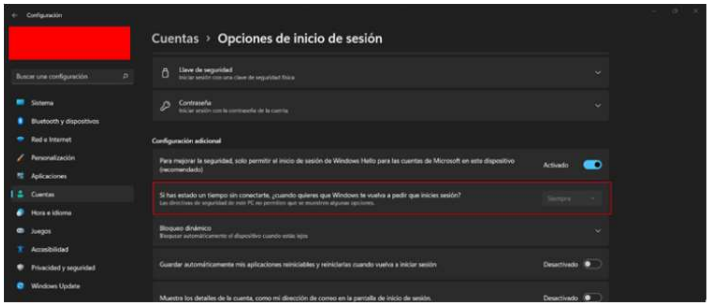
En Windows

- Desde el menú '**Inicio**', haz clic encima de tu nombre de usuario y luego en '**Bloquear**'.
- Usando el atajo de teclado Windows + L desde cualquier pantalla.
- Para portátiles, configura la suspensión cuando se cierra la tapa. Abre el menú '**Inicio**' y escribe '**Panel de control**'. Ábrelo y ve a '**Hardware y sonido**' > '**Opciones de energía**', y en esta ventana haz clic en '**Elegir el comportamiento del cierre de la tapa**' en la izquierda de la pantalla. Ahora configura las dos opciones marcadas en la imagen en '**Suspender**'.



- Por tiempo de inactividad, ve a '**Configuración**' > '**Sistema**' > '**Energía y batería**'. En esta página, puedes configurarlo en '**Pantalla y suspensión**'.

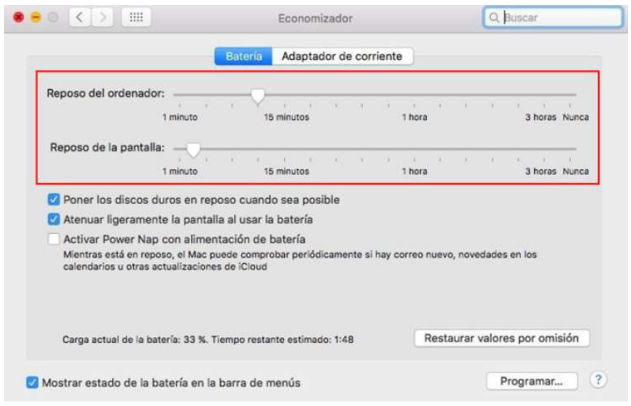
También es recomendable forzar que Windows pida la contraseña siempre tras el reposo. Ajustando la siguiente opción en '**Configuración**' > '**Cuentas**' > '**Opciones de inicio de sesión**'.



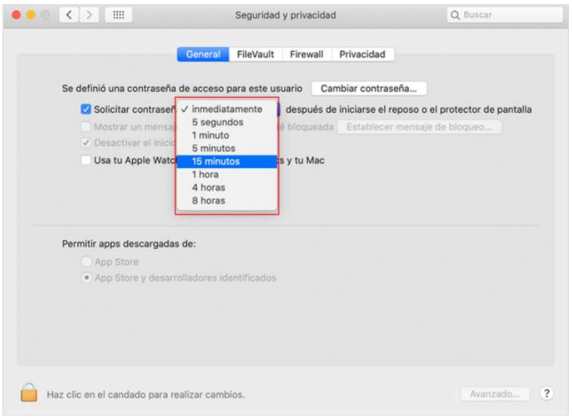
En Mac

- Con el atajo de teclado Control + Comando + Q.
- Desde el menú Apple, y 'Bloquear pantalla'.
- Por tiempo de inactividad.

Ve a '**Preferencias del sistema**' > '**Economizador**'. En la pestaña '**Batería**' configura el tiempo de reposo.



También puedes habilitar la opción para que se solicite la contraseña siempre después del reposo, en '**Preferencias del sistema**' > '**Seguridad y privacidad**', en la pestaña '**General**'



5. Usa programas antivirus de confianza y mantén actualizadas las definiciones de virus.

Asegúrate siempre de usar programas antivirus de confianza y reconocidos, ya que esto asegura una mejor protección.

Escoge aquellos que ofrezcan una protección completa, tanto del equipo como del navegador web. Los sistemas operativos modernos ya incorporan medidas de protección contra *malware* y modificaciones.

Mantén siempre actualizadas las definiciones de virus para mantener tu equipo protegido. Esto puedes hacerlo desde el apartado de actualizaciones del sistema operativo o desde el antivirus, según el programa que estés usando.

En nuestra web encontrarás algunas herramientas antivirus gratuitas que te pueden interesar.

6. Desinstala las aplicaciones basura que vienen preinstaladas y aquellas que no vayas a utilizar.

Por defecto, los sistemas operativos traen muchas aplicaciones preinstaladas que son poco útiles o no vamos a usar. Es recomendable desinstalarlas por seguridad, ya que pueden contener vulnerabilidades y al no usarlas, se nos olvide actualizarlas dejando una puerta de entrada para los cibercriminales.

7. Revisa las opciones de privacidad y configúralas según tus necesidades.

Las opciones de privacidad son importantes, porque de esa manera determinamos cómo queremos que las aplicaciones usen nuestros datos, recopilen información y también cómo se envían las estadísticas de uso que recoge el sistema.

En Windows

Ve a '**Configuración**' > '**Privacidad y seguridad**'

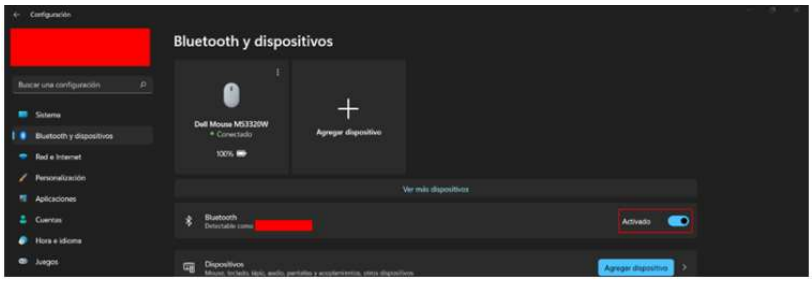
En Mac

Ve a '**Preferencias del sistema**' > '**Seguridad y privacidad**'.

8. Deshabilita la conexión Bluetooth y wifi cuando no la uses.

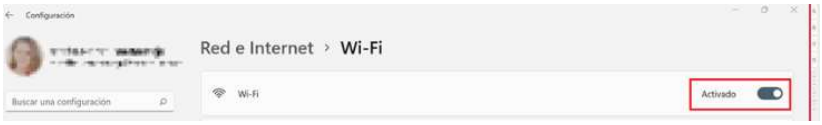
Las conexiones Bluetooth son otro tipo de conexión inalámbrica y, por tanto, otro punto de entrada a nuestros computadores.

En Windows



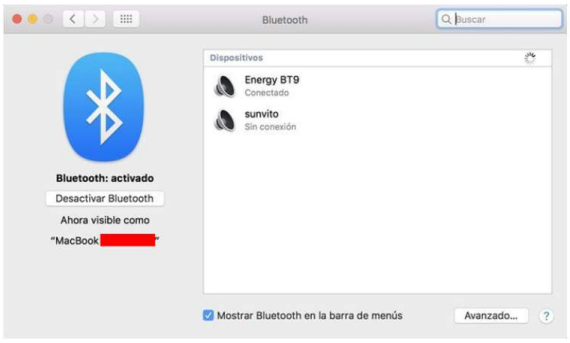
Ve a '**Configuración**' > '**Bluetooth y dispositivos**'. Deshabilita la opción que marca la imagen.

Para deshabilitar el wifi, ve a '**Configuración**' > '**Red e Internet**' y apágalo.

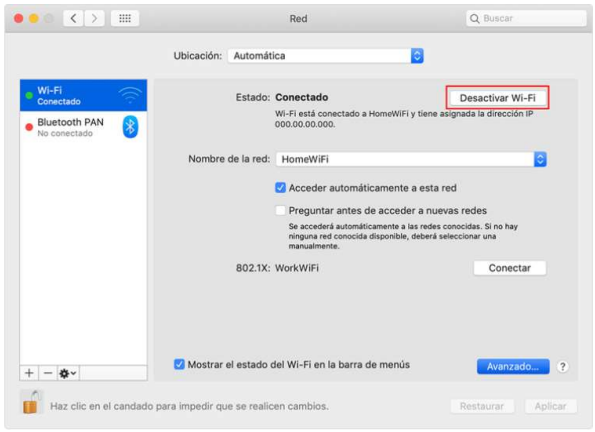


En Mac

Ve a '**Preferencias del sistema**' > '**Bluetooth**'.



Ve a '**Preferencias del sistema**' > '**Red**' > '**Wi-Fi**'



9. Activa el cortafuegos (firewall).

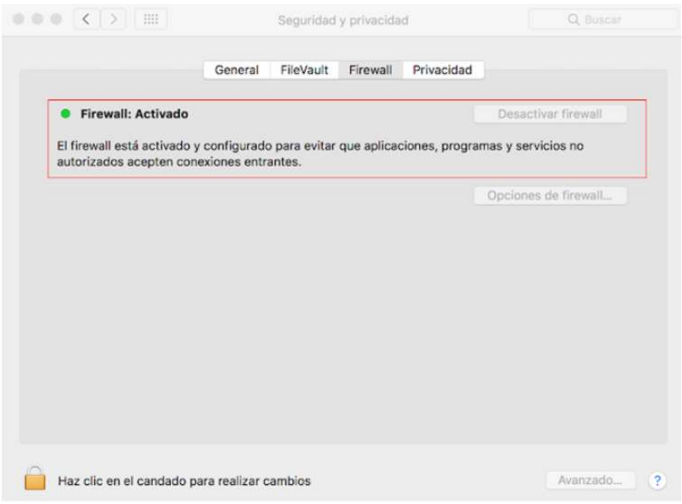
El firewall, es un programa que actúa como un muro que nos protege de intrusiones. Por ello, hay que revisar que está activado y bien configurado.

En Windows

Podemos ver su estado en '<u>Seguridad de Windows</u>', en la pestaña '**Firewall y protección de red**'.

En Mac

Ve a '**Preferencias del sistema**' > '**Seguridad y privacidad**', en la pestaña 'Firewall'.

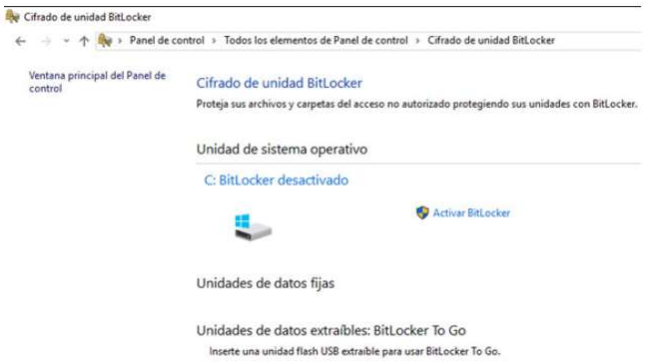


10. Habilita el cifrado de disco.

El cifrado de disco, asegura que los datos que tenemos en el computador no son legibles a terceras personas que tengan acceso a nuestro equipo.

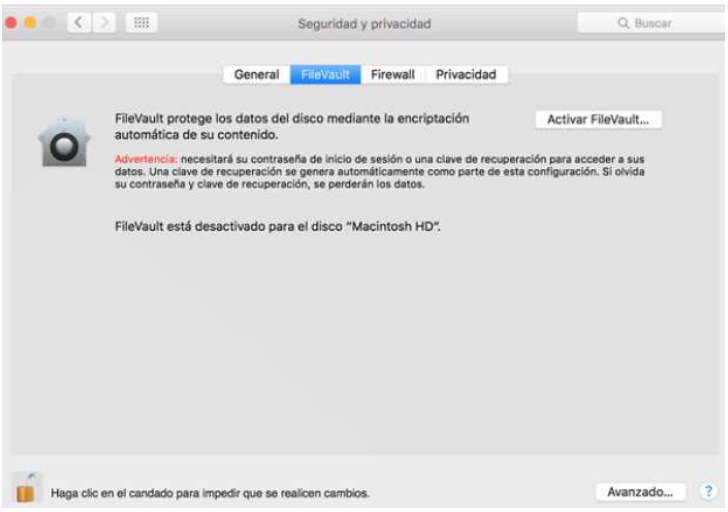
En Windows

Podemos configurar **BitLocker** para el cifrado. Para ello, abre el '**Panel de control**', y ve a '**Sistema y seguridad**' > '**Cifrado de unidad BitLocker**'.



En Mac

En Mac tenemos la función **FileVault**. Podemos encontrarlo en '**Preferencias del sistema**' > '**Seguridad y privacidad**', en la pestaña '**FileVault**'.



AUTOR:

INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD)

ENLACE:

https://www.osi.es/es/actualidad/blog/2023/01/12/10-consejos-para-proteger-tu-nuevo-ordenador