10 consellos para protexer o teu novo computador

Compráches un novo computador e acaba de chegarche? Queres saber cal pode ser a mellor forma de mantelo seguro, e de protexer os teus datos? Neste artigo, explicámosche algúns pasos para que poidas configuralo da mellor maneira co obxectivo de mantelo seguro.

Na actualidade, non é estraño que teñamos en casa un ou máis ordenadores. Baseamos unha parte da nosa vida nestes dispositivos, así que é moi importante que saibamos como protexer os datos que gardamos neles.

Por ese motivo, proporcionámosche os seguintes consellos para axudarche nesta importante tarefa. Sígueos e protéxeche!

Que che recomendamos?

1. Mantén o teu equipo actualizado coas últimas actualizacións dispoñibles.

2. Protexe a túa conta de usuario cun contrasinal robusta.

3. Deshabilita o inicio de sesión automático.

4. Configura o bloqueo do equipo cando estás ausente ou entra en repouso

5. Usa programas antivirus de confianza e mantenlo actualizado.

6. Desinstala as aplicacións lixo que veñen preinstaladas e aquelas que non vaias utilizar.

7. Revisa as opcións de privacidade e configúraas segundo as túas necesidades.

8. Deshabilita a conexión wifi e Bluetooth cando non a uses.

9. Activa a devasa (firewall).

10. Habilita o cifrado de disco.

Como podes facelo?

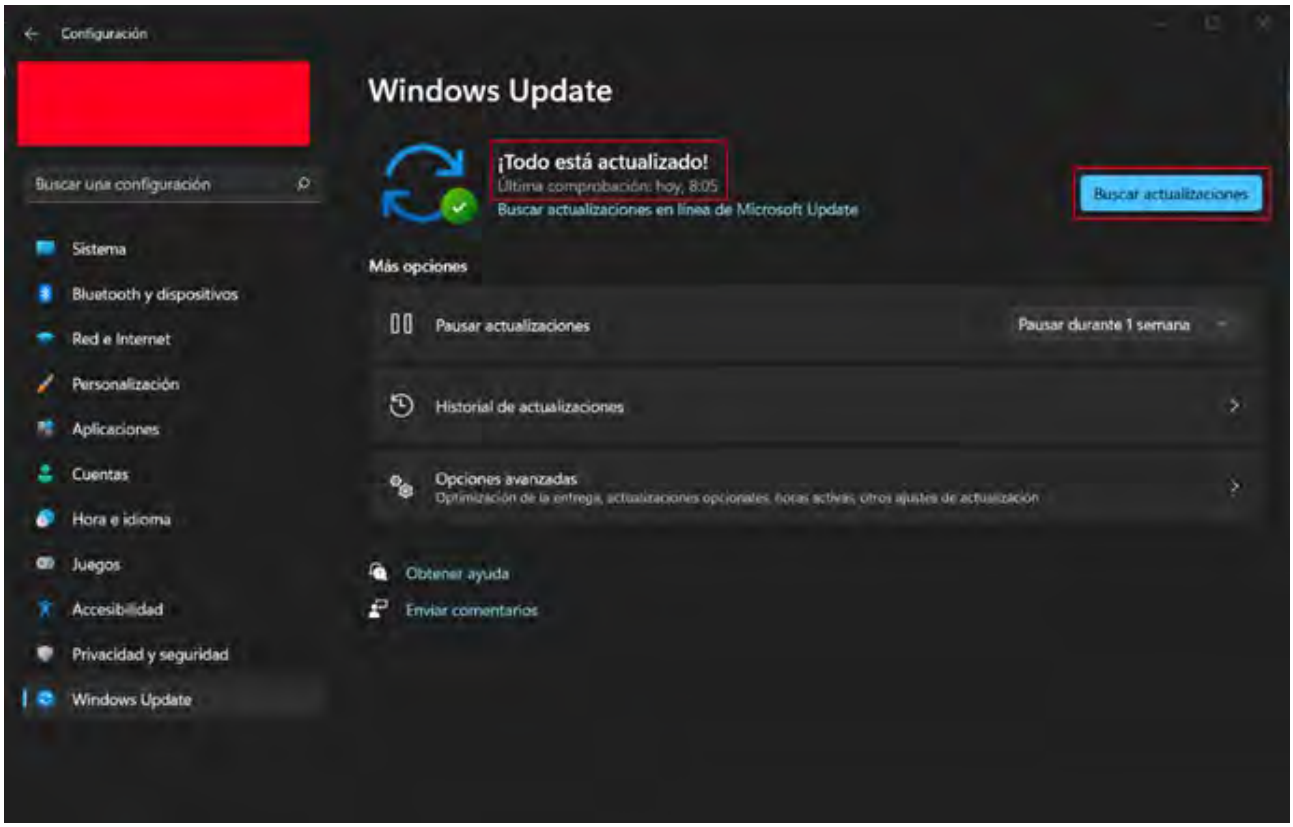
1. Mantén o teu equipo actualizado coas últimas actualizacións dispoñibles.

É moi importante manter actualizado o sistema operativo, controladores e aplicacións do noso computador, xa que as actualizacións melloran o rendemento e corrixen vulnerabilidades.

En Windows

Abre a aplicación de **'Configuración'** desde o menú 'Inicio', ve a **'Windows Update'** e pulsa no botón **'Buscar actualizacións'** para ver se hai novas actualizacións dispoñibles.

En caso de non haber actualizacións, aparecerá a mensaxe **'Todo está actualizado!'**.



En caso de haber novas actualizacións, aparecería como na seguinte imaxe, co mensaxe '**Actualizacións dispoñibles para instalar**' e fariamos clic en **'Instalar agora'**.

Unha vez instaladas, pedirache reiniciar o computador para aplicar as actualizacións, podemos facer clic en '**Reiniciar agora**' para iso.

En Mac

No menú Apple (na esquina superior esquerda da pantalla), entra a '**Preferencias do sistema**' > **'Actualización de software'.** Se hai algunha actualización dispoñible, fai clic en **'Actualiza agora'** para instalala.

2. Protexe a túa conta de usuario cun contrasinal robusta.

Para que un contrasinal sexa forte, debe cumprir:

- Ter unha lonxitude mínima de 8 caracteres.
- Conter caracteres alfanuméricos (letras minúsculas, maiúsculas e números).
- Conter caracteres especiais ($, #, &, etc.).
- Non ten que conter datos persoais, como datas relevantes, nomes propios...

En Windows

Ve a **'Configuración'** > **'Contas'** > **'Opcións de inicio de sesión'**. No apartado **'Contrasinal'** poderás poñer unha ou cambiala, se xa o facías.

En Mac

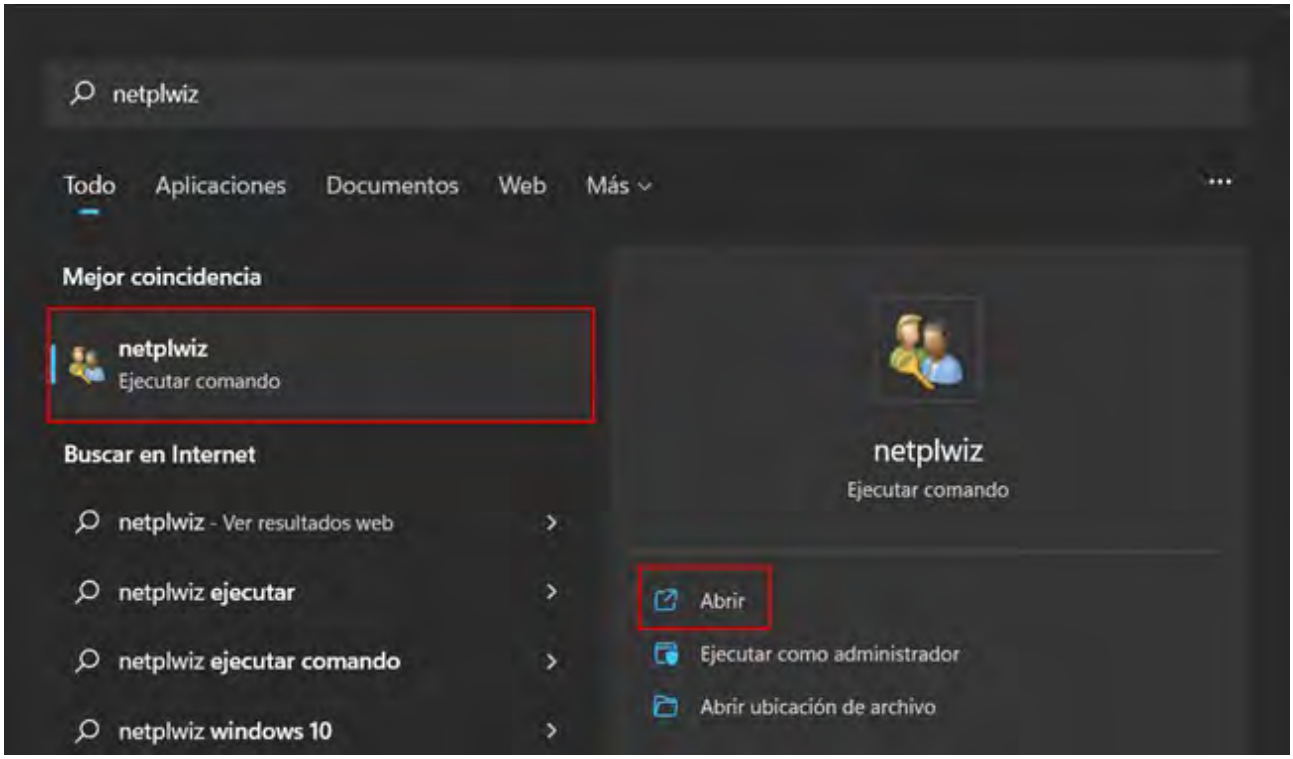
Ve a '**Preferencias do sistema** > **'Usuarios e grupos'**. Aquí selecciona o teu usuario e fai clic en **'Cambiar contrasinal'**.

3. Deshabilita o inicio de sesión automático.

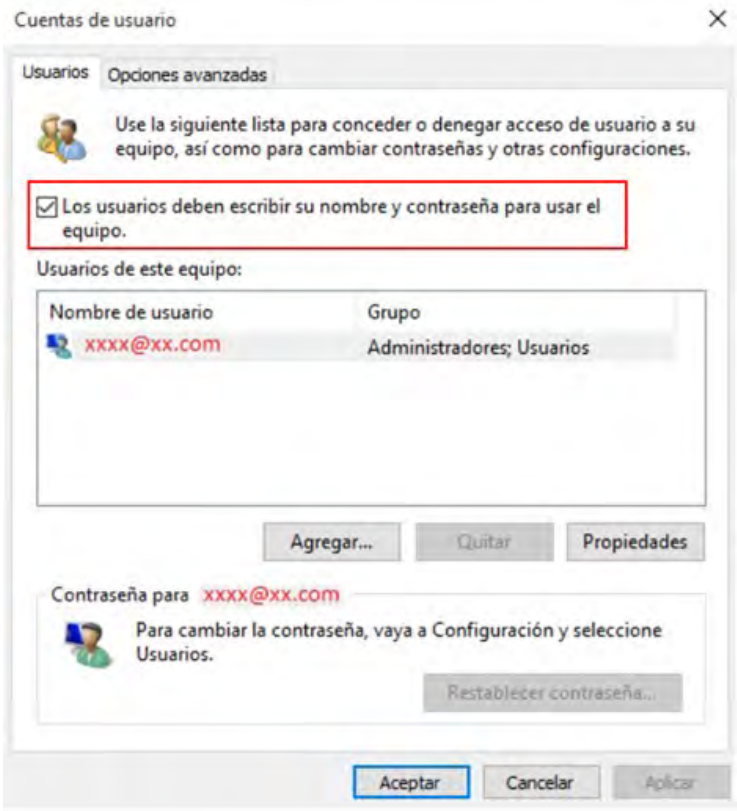
Se somos os únicos que usamos o noso computador, é bastante cómodo, que queiramos habilitar o inicio automático de sesión. Esta práctica é perigosa porque calquera persoa que teña acceso ao equipo, poderá iniciar sesión nel e chegar así aos nosos datos. Por iso, o mellor é comprobar se esta opción está desactivada.

En Windows

Para comprobalo, abre o menú Inicio e no campo de procura escribe **'netplwiz'**. Fai clic sobre a aplicación que aparece na seguinte imaxe.

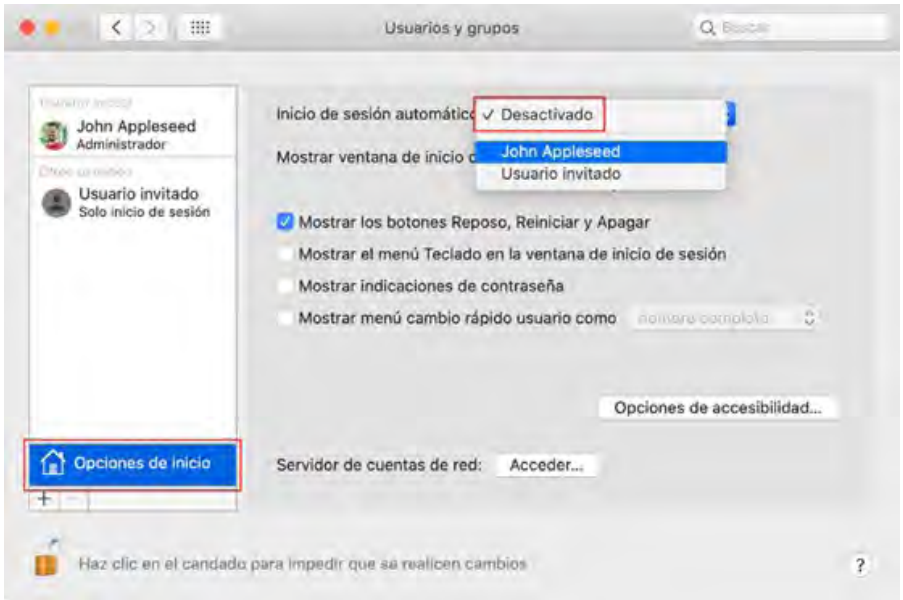


Unha vez ábrase a xanela, como na seguinte imaxe, asegúrache que a casa **'Os usuarios deben escribir o seu nome e contrasinal para usar o equipo'** estea marcada, antes de pechar a xanela e non esquezas **'Aplicar os cambios'**.



En Mac

Ve a **'Preferencias do sistema'** > **'Usuarios e grupos'**. Fai clic na icona do cadeado (na parte inferior da xanela) e escribe o contrasinal da conta. Fai clic en **'Opcións de inicio'**, na esquina inferior esquerda, e asegúrache de seleccionar a opción **'Desactivado'** no menú despregable **'Inicio de sesión automático'**.



4. Configura o bloqueo automático do equipo cando estás ausente ou entra en repouso.

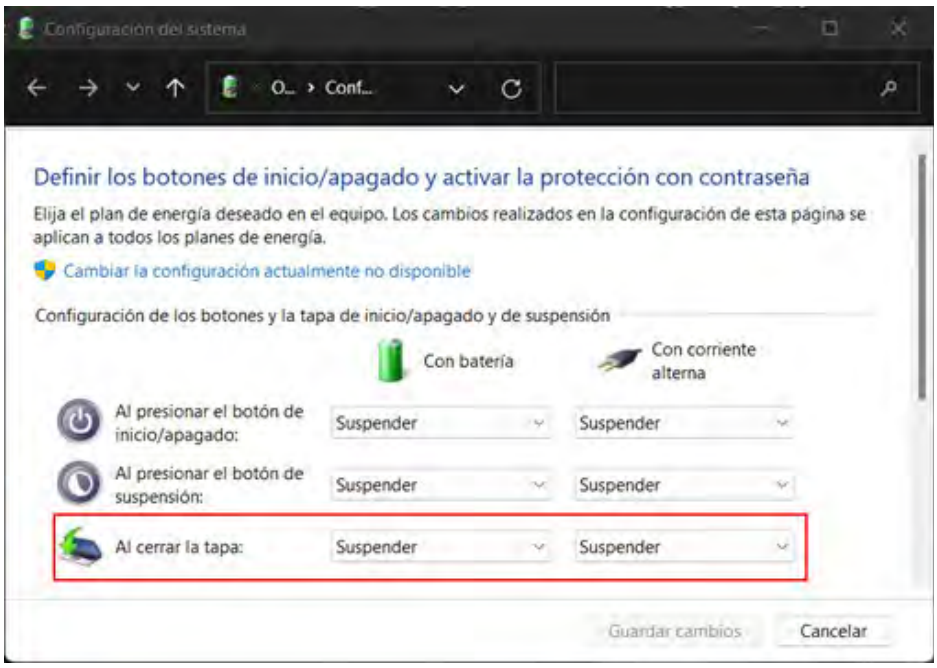
Cando te levantes para descansar ou non vaias utilizar o computador nun intre, é importante bloquealo, para que outras persoas non teñan acceso a el.

Os seguintes casos, son exemplos de cando se bloquea o equipo:

- Deixar de teclear e usar o rato por un tempo definido segundo os axustes.
- Ter un computador portátil e pechar a tapa.
- Bloquéase manualmente.

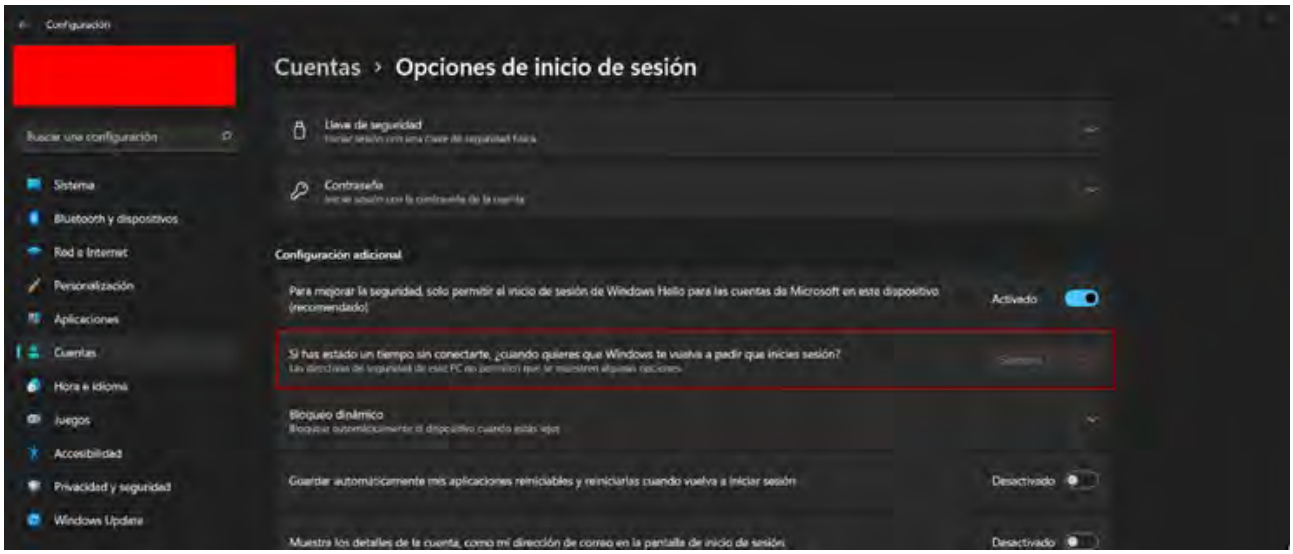
En Windows

- Desde o menú '**Inicio**', faise clic encima do teu nome de usuario e logo en '**Bloquear**'.
- Usando o atallo de teclado Windows + L desde calquera pantalla.
- Para portátiles, configura a suspensión cando se pecha a tapa. Abre o menú '**Inicio**' e escribe '**Panel de control**'. Ábreo e ve a '**Hardware e son**' > '**Opcións de enerxía**', e nesta xanela fai clic en '**Elixir o comportamento do peche da tapa**' na esquerda da pantalla. Agora configura as dúas opcións marcadas na imaxe en '**Suspender**'.



- Por tempo de inactividade, ve a '**Configuración**' > '**Sistema**' > '**Enerxía e batería**'. Nesta páxina, podes configuralo en '**Pantalla e suspensión**'.

Tamén é recomendable forzar que Windows pida o contrasinal sempre tras o repouso. Axustando a seguinte opción en '**Configuración**' > '**Contas**' > '**Opcións de inicio de sesión**'.

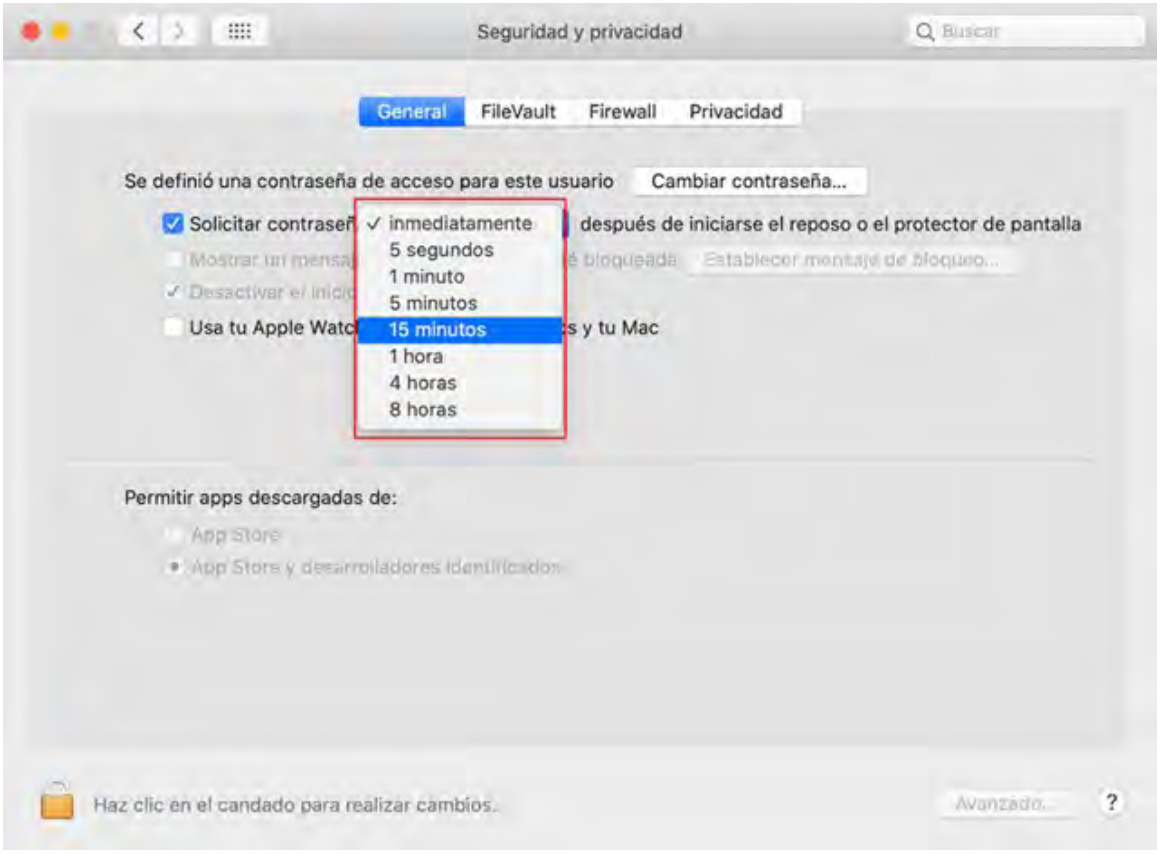


En Mac

- Co atallo de teclado Control + Comando + Q.
- Desde o menú Apple, e 'Bloquear pantalla'.
- Por tempo de inactividade.

Ve a '**Preferencias do sistema**' > '**Economizador**'. Na pestana '**Batería**' configura o tempo de repouso.

Tamén podes habilitar a opción para que se solicite o contrasinal sempre despois do repouso, en '**Preferencias do sistema**' > '**Seguridade e privacidade'**, na pestana '**Xeral**'



5. Usa programas antivirus de confianza e mantén actualizadas as definicións de virus.

Asegúrache sempre de usar programas antivirus de confianza e recoñecidos, xa que isto asegura unha mellor protección.

Escolle aqueles que ofrezan unha protección completa, tanto do equipo como da navegador web. Os sistemas operativos modernos xa incorporan medidas de protección contra malware e modificacións.

Mantén sempre actualizadas as definicións de virus para manter o teu equipo protexido. Isto podes facelo desde o apartado de actualizacións do sistema operativo ou desde o antivirus, segundo o programa que esteas a usar.

Na nosa web atoparás algunhas ferramentas antivirus gratuítas (https://www.osi.es/es/herramientas) que che poden interesar.

6. Desinstala as aplicacións lixo que veñen preinstaladas e aquelas que non vaias utilizar.

Por defecto, os sistemas operativos traen moitas aplicacións preinstaladas que son pouco útiles ou non imos usar. É recomendable desinstalarlas por seguridade, xa que poden conter vulnerabilidades e ao non usalas, esquézasenos actualizalas deixando unha porta de entrada para os cibercriminales.

7. Revisa as opcións de privacidade e configúraas segundo as túas necesidades.

As opcións de privacidade son importantes, porque dese xeito determinamos como queremos que as aplicacións usen os nosos datos, recompilen información e tamén como se envían as estatísticas de uso que recolle o sistema.

En Windows

Ve a '**Configuración**' > '**Privacidade e seguridade**'

En Mac

Ve a '**Preferencias do sistema**' > '**Seguridade e privacidade**'.

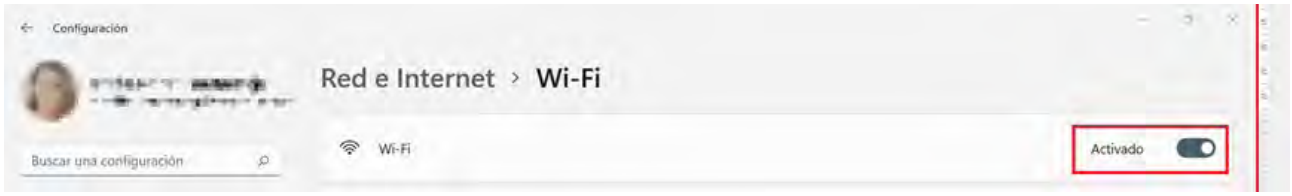
8. Deshabilita a conexión Bluetooth e wifi cando non a uses.

As conexións Bluetooth son outro tipo de conexión inalámbrica e, por tanto, outro punto de entrada aos nosos computadores.

En Windows

Ve a '**Configuración**' > '**Bluetooth e dispositivos'**. Deshabilita a opción que marca a imaxe.

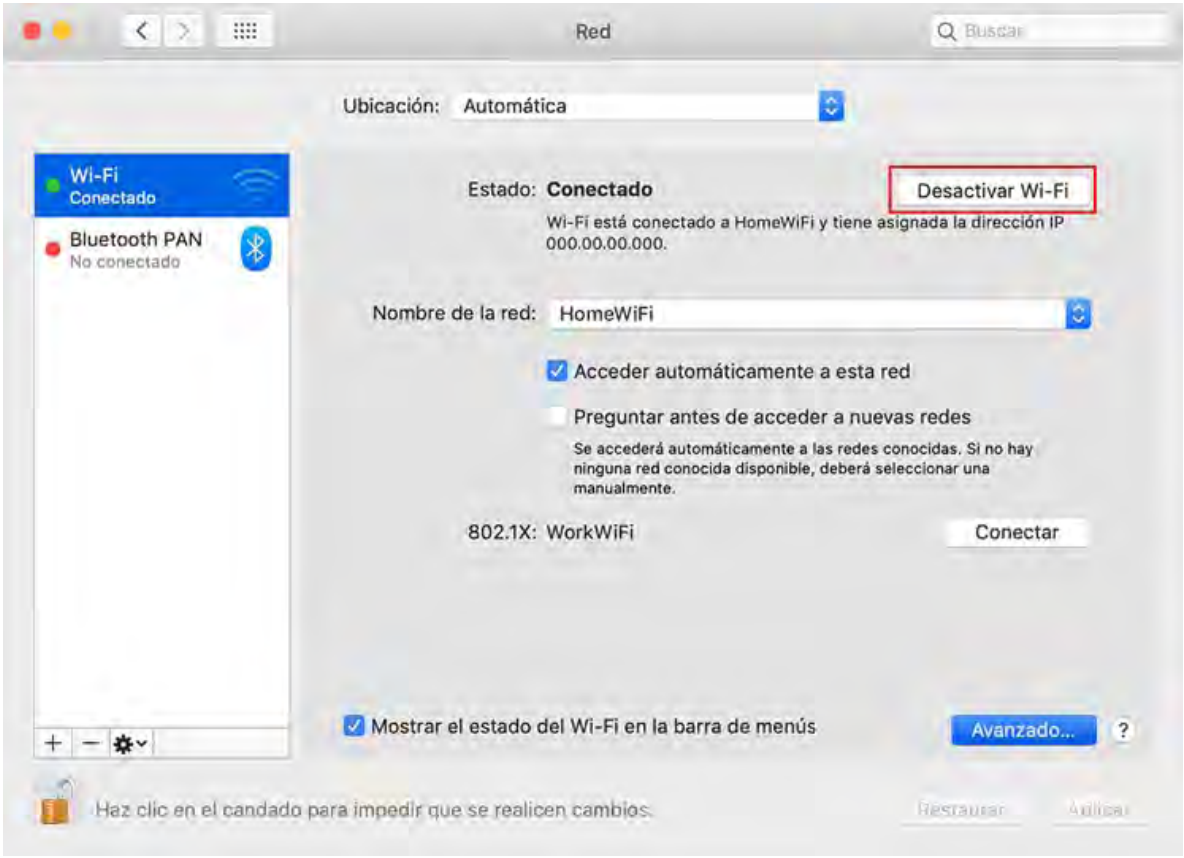
Para deshabilitar o wifi, ve a '**Configuración**' > '**Rede e Internet**' e apágao.



En Mac

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

Ve a '**Preferencias do sistema**' > '**Rede**' > '**Wi-fi**'



9. Activa a devasa (firewall).

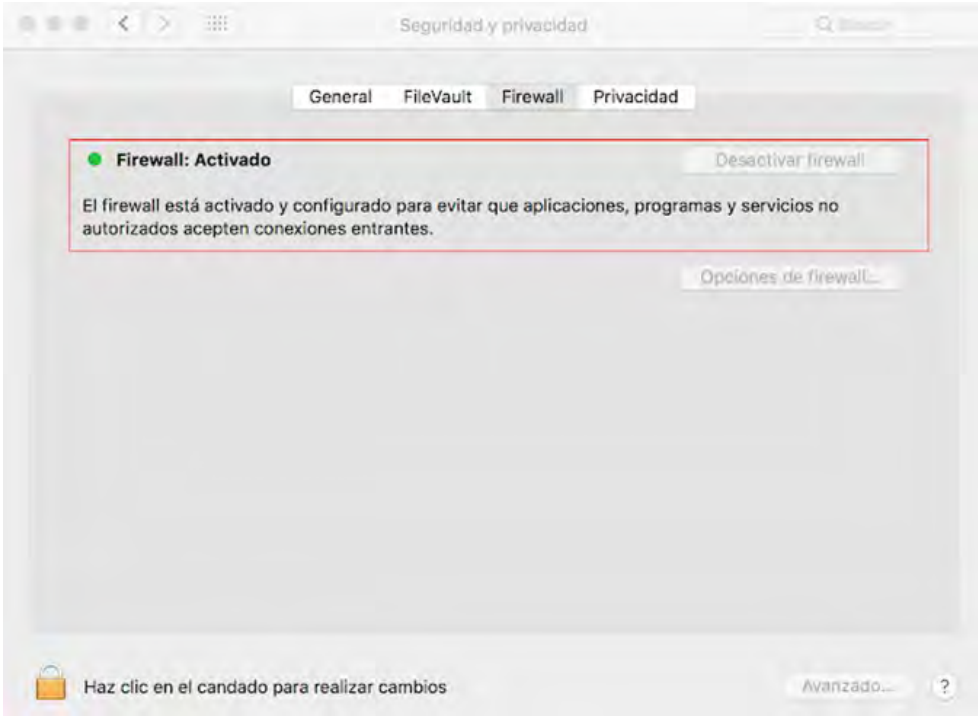
O firewall, é un programa que actúa como un muro que nos protexe de intrusións. Por iso, hai que revisar que está activado e ben configurado.

En Windows

Podemos ver o seu estado en '**Seguridade de Windows**', na pestana '**Firewall e protección de rede**'.

En Mac

Ve a '**Preferencias do sistema**' > '**Seguridade e privacidade**', na pestana '**Firewall**'.



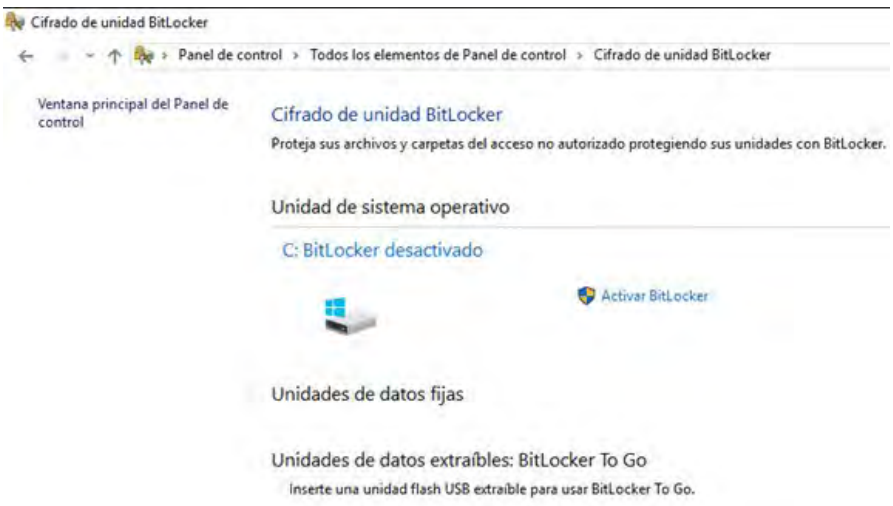
10. Habilita o cifrado de disco.

O cifrado de disco, asegura que os datos que temos no computador non son lexibles a terceiras persoas que teñan acceso ao noso equipo.

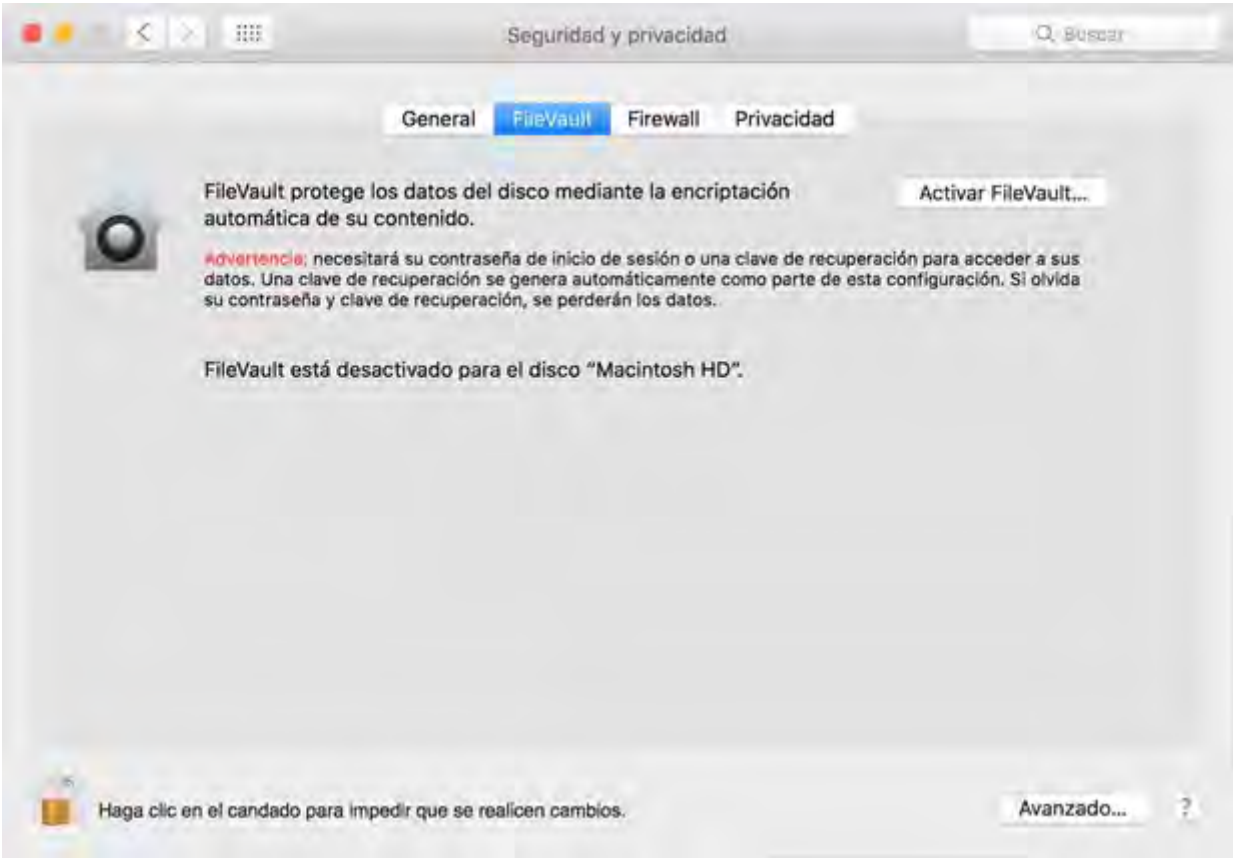
En Windows

Podemos configurar BitLocker para o cifrado. Para iso, abre o '**Panel de control**', e ve a '**Sistema e seguridade**' > '**Cifrado de unidade BitLocker**'.

En Mac



En Mac temos a función FileVault. Podemos atopalo en '**Preferencias do sistema**' > '**Seguridade e privacidade**', na pestana '**FileVault**'.



Como sempre dicimos, as novas tecnoloxías ofrecen moitas posibilidades, e estando informados, podemos ter a configuración máis segura dos nosos dispositivos para a nosa protección e a dos nosos seres queridos. Ademais, contas coa Liña de Axuda en Ciberseguridade de INCIBE (https://www.incibe.es/linea-de-ayuda-en-ciberseguridad), 017, gratuíta e confidencial, para consultar as túas dúbidas e problemas sempre que o necesites. Tamén por WhatsApp 900 116 117 ou Telegram @INCIBE017.

Fonte: Oficina de Seguridad del Internauta (OSI)