INSTITUTO NACIONAL DE CIBERSEGURIDAD

https://www.osi.es/es

Oficina de Seguridad del Internauta de INCIBE

10 consejos para proteger tu nuevo ordenador

Publicado el
12/01/2023

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

¿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 cortafuegos (*firewall*).
10. Habilita el cifrado de disco.

¿Cómo puedes hacerlo?

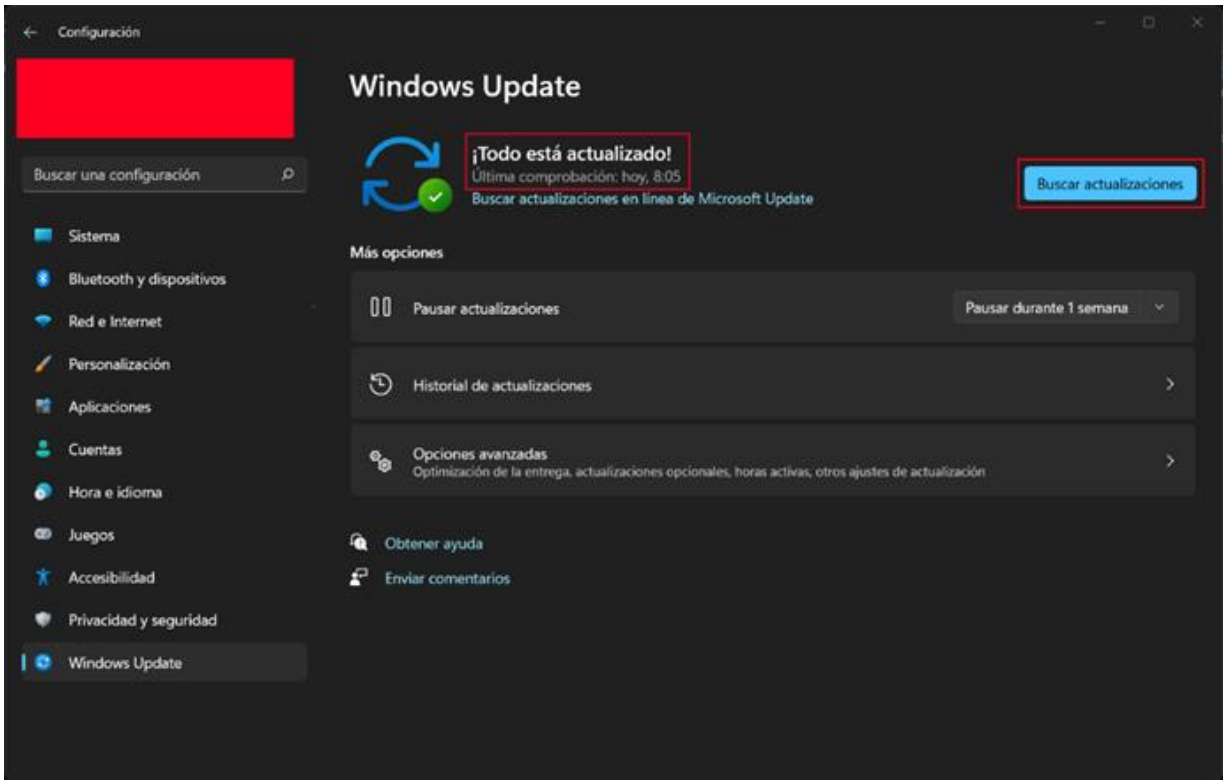
1. Mantén tu equipo actualizado con las últimas actualizaciones disponibles.

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

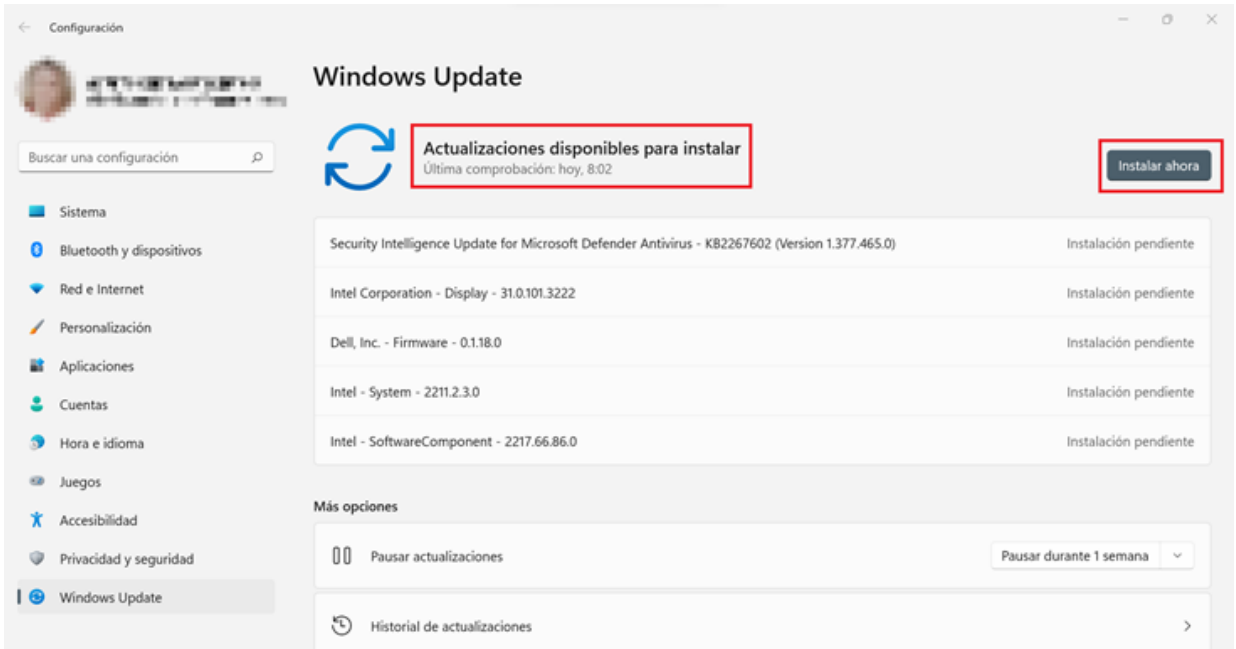
En Windows

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 ordenador 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:

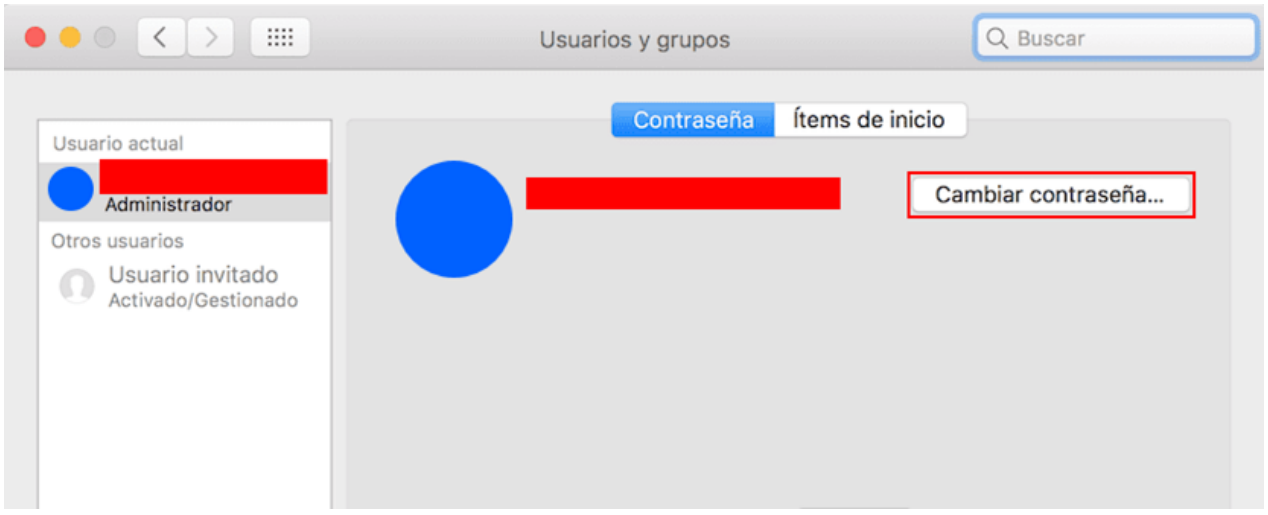
- Tener una longitud mínima de 8 caracteres.
- Contener caracteres alfanuméricos (letras minúsculas, mayúsculas y números).
- Contener caracteres especiales ($, #, &, etc.).
- No tiene que contener datos personales, como fechas relevantes, nombres propios…

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**'.

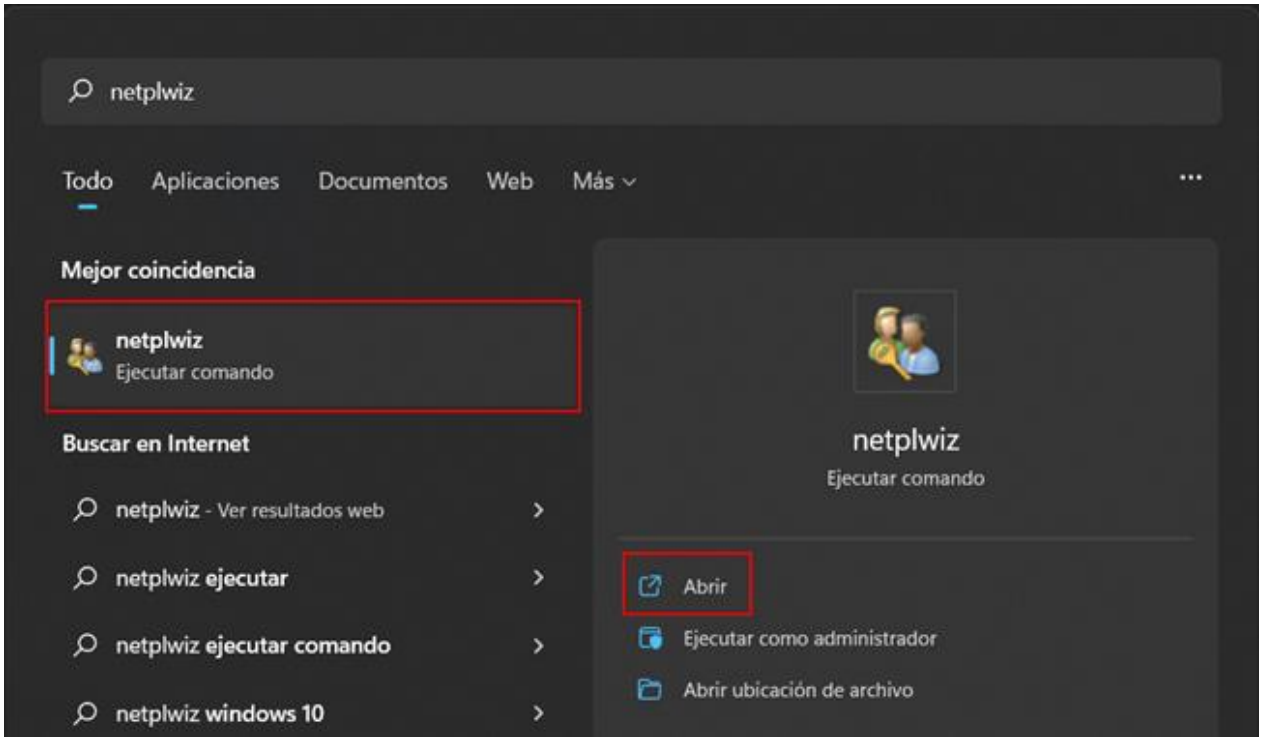


3. Deshabilita el inicio de sesión automático.

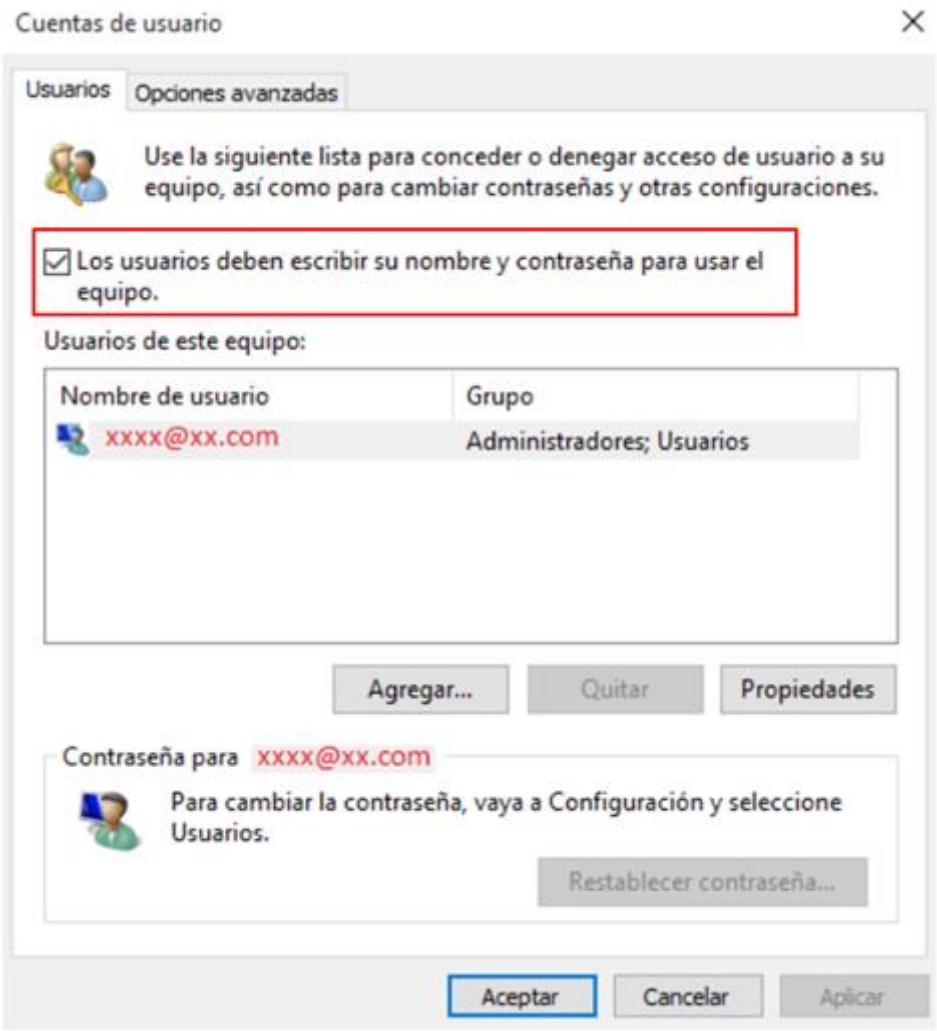
Si somos los únicos que usamos nuestro ordenador, es bastante cómodo, que queramos habilitar el inicio automático de sesión. Esta práctica es peligrosa porque cualquier persona que tenga acceso al equipo, podrá iniciar sesión en él y llegar así a nuestros datos. Por eso, lo mejor es comprobar si esta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

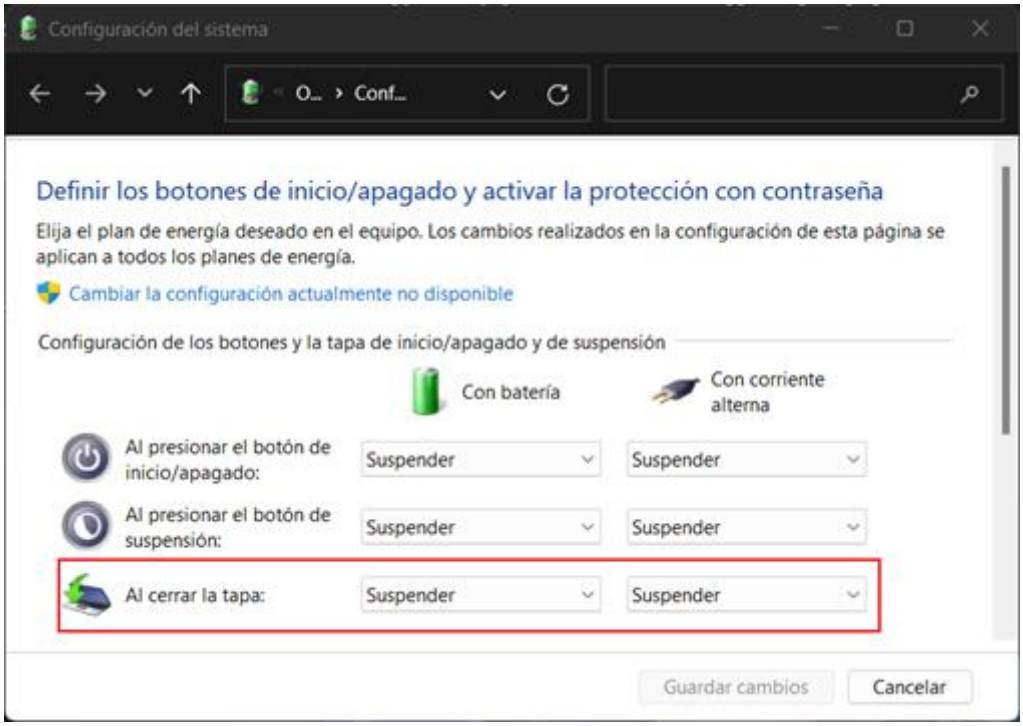
Cuando te levantes para descansar o no vayas a utilizar el ordenador en un rato, es importante bloquearlo, para que otras personas no tengan acceso a él.

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 ordenador portátil y cerrar la tapa.
- Se bloquea manualmente.

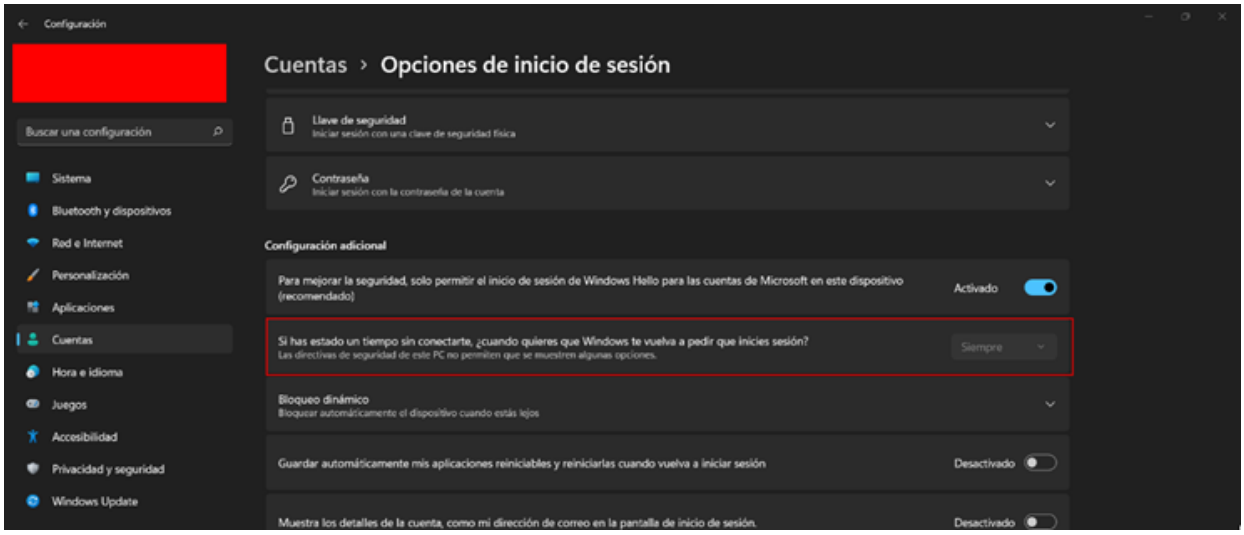
En Windows

- 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**'.

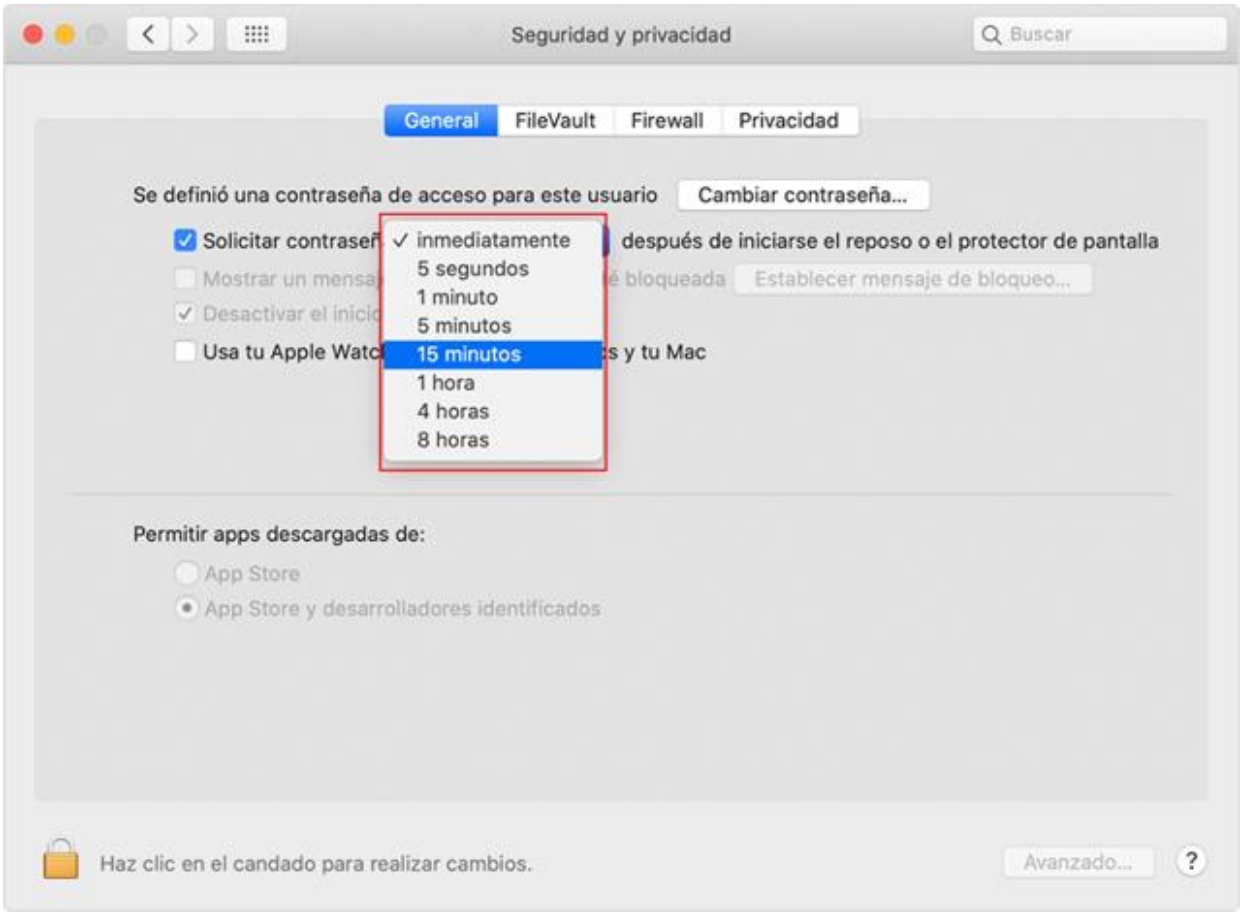


En Mac

- 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.

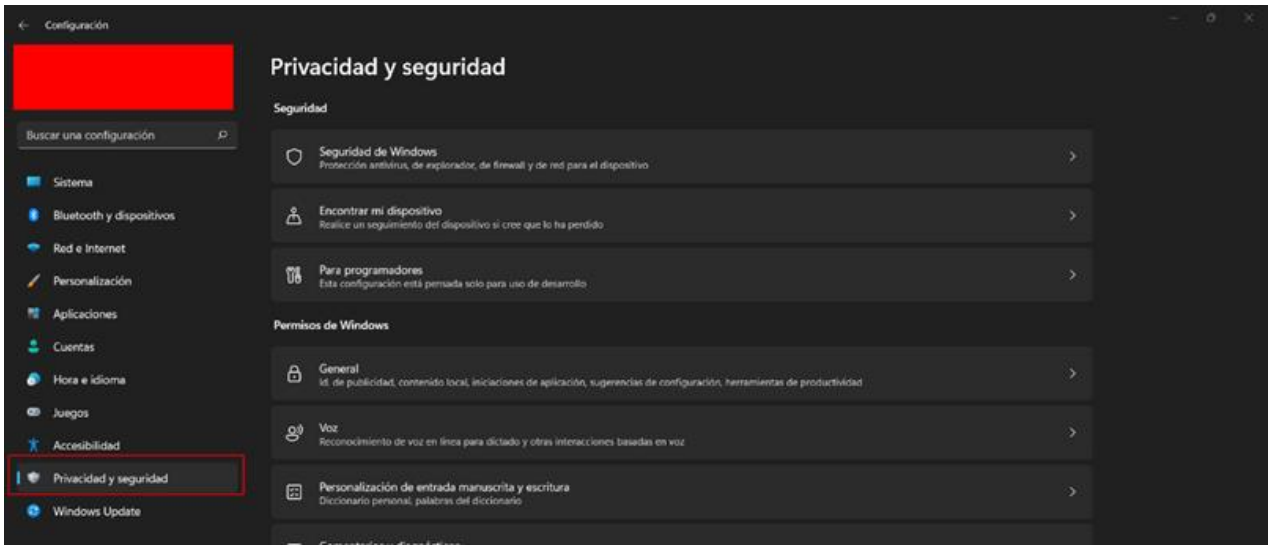
Por defecto, los sistemas operativos traen muchas aplicaciones preinstaladas que son poco útiles o no vamos a usar. Es recomendable desinstalarlas por seguridad, ya que pueden contener vulnerabilidades y al no usarlas, se nos olvide actualizarlas dejando una puerta de entrada para los cibercriminales.

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**'.

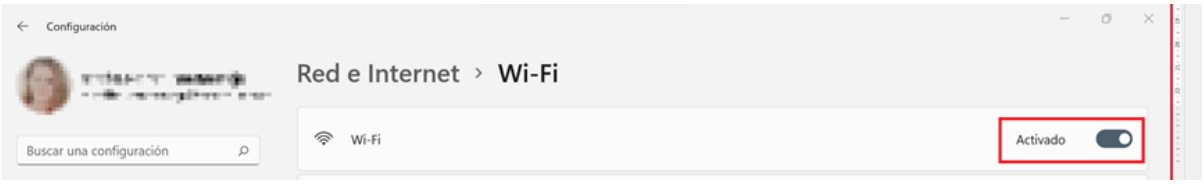
8. Deshabilita la conexión Bluetooth y wifi cuando no la uses.

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

En Windows

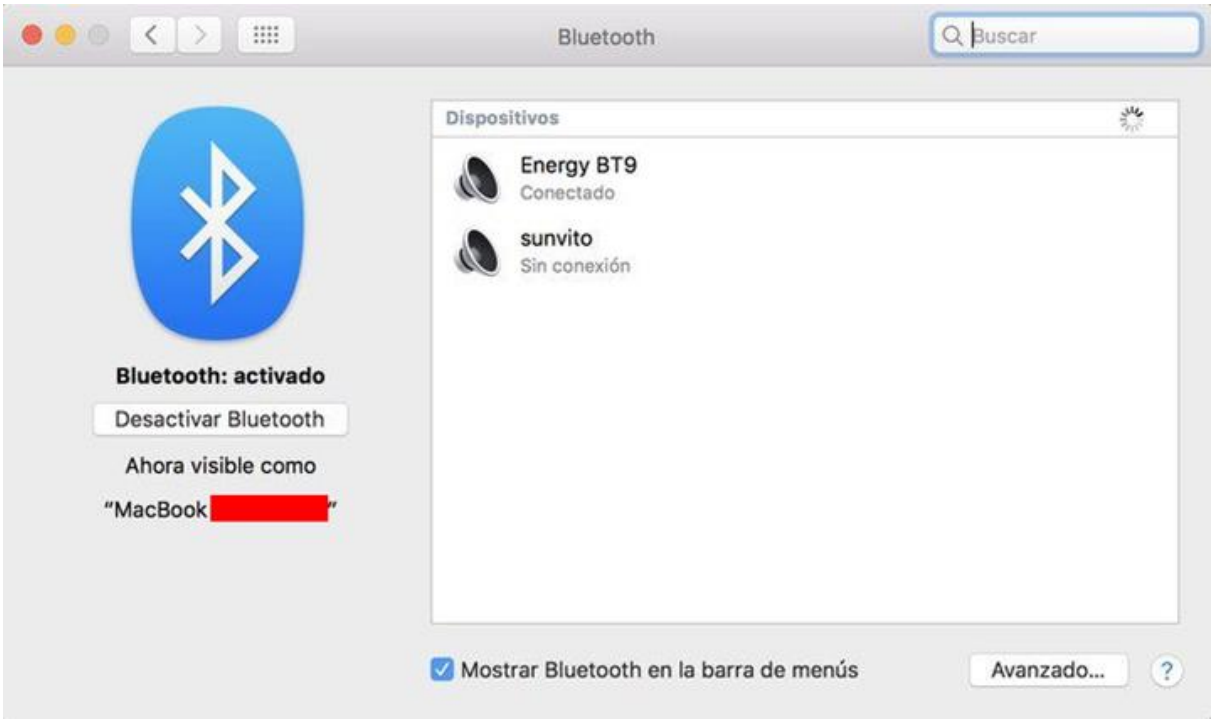
Ve a '**Configuración**' > '**Bluetooth y dispositivos**'. Deshabilita la opción que marca la imagen.

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

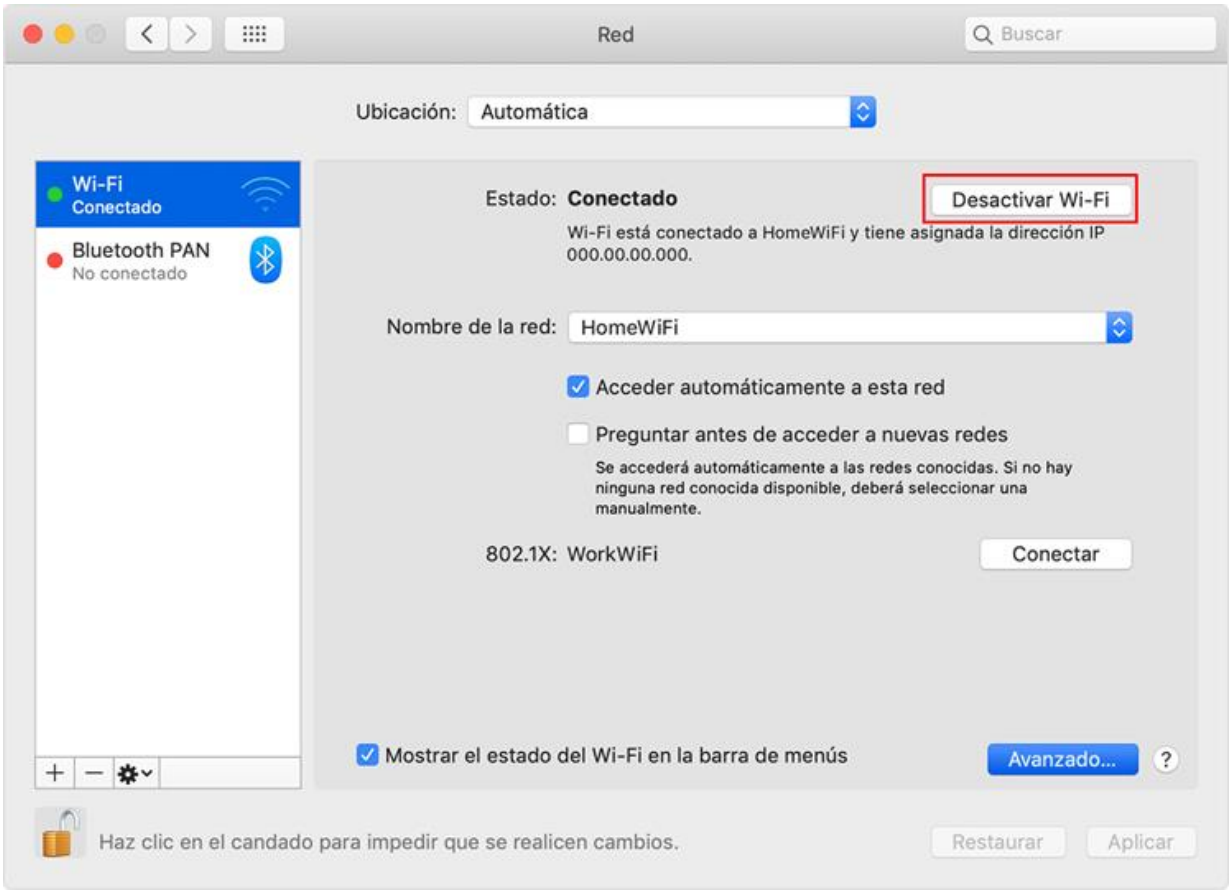


En Mac

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



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



9. Activa el cortafuegos (firewall).

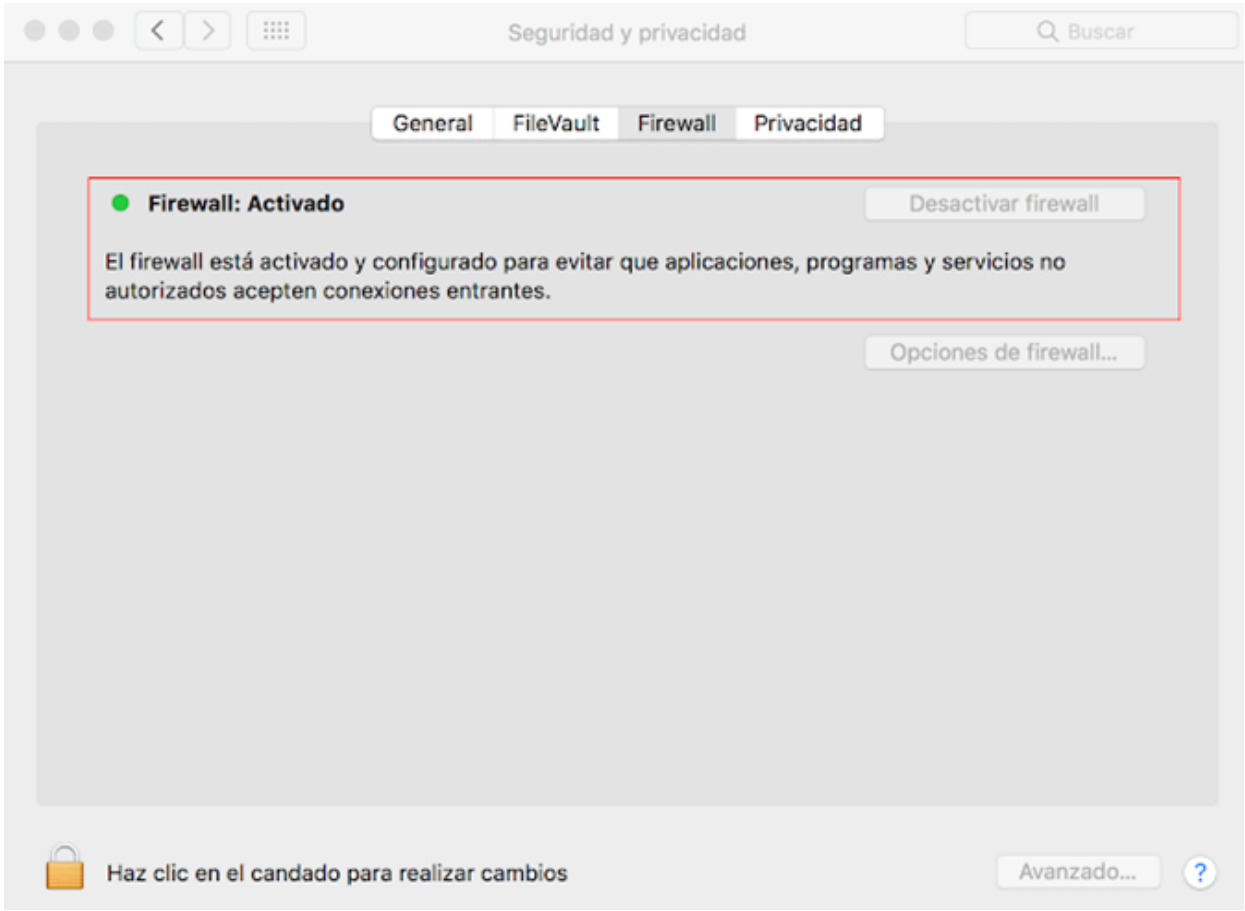
El firewall, es un programa que actúa como un muro que nos protege de intrusiones. Por ello, hay que revisar que está activado y bien configurado.

En Windows

Podemos ver su estado en '[Seguridad de Windows]', en la pestaña '**Firewall y protección de red**'.

En Mac

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

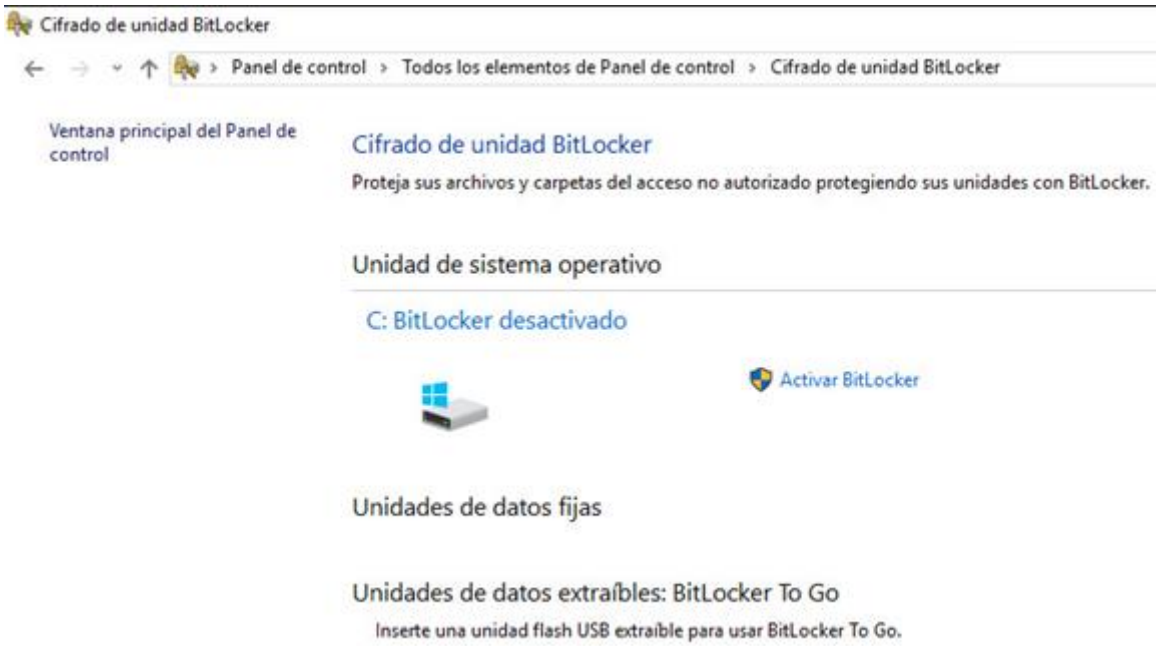


10. Habilita el cifrado de disco.

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

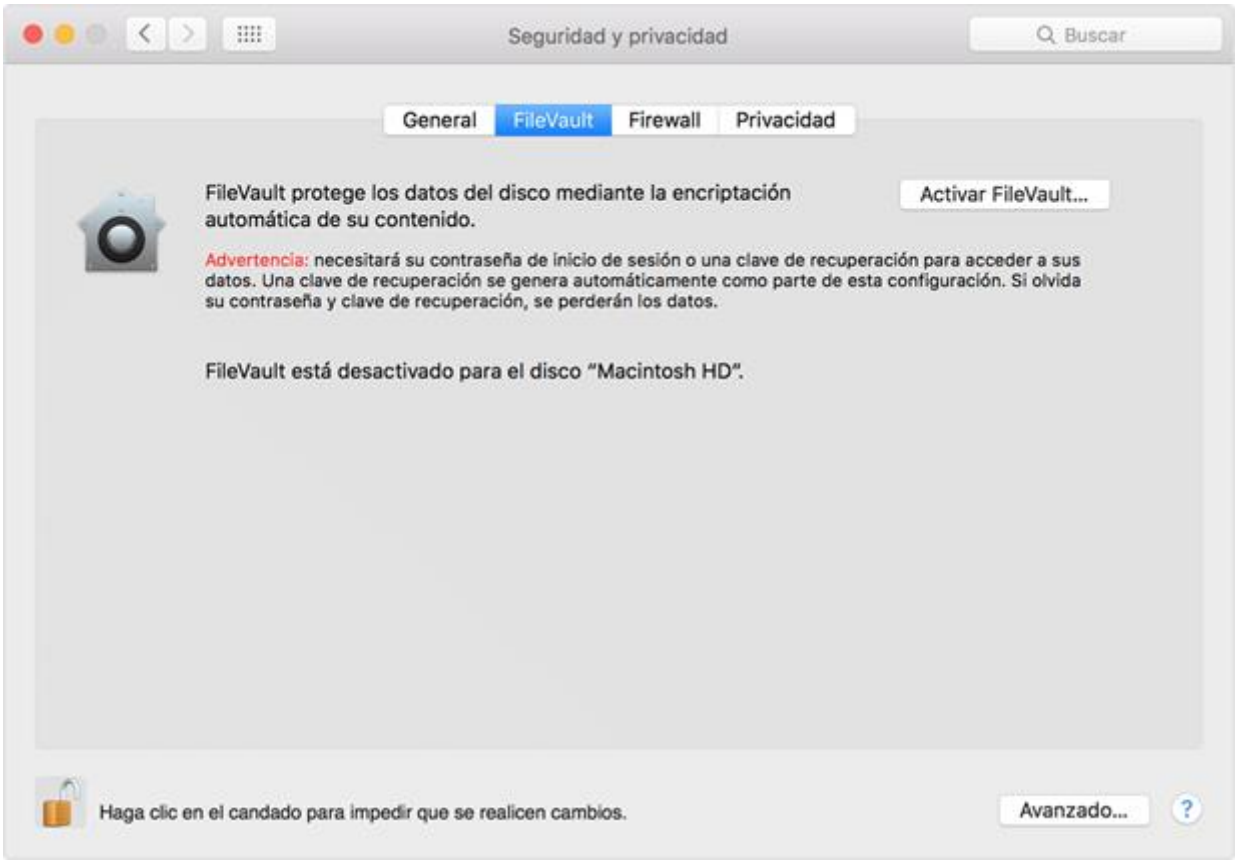
En Windows

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

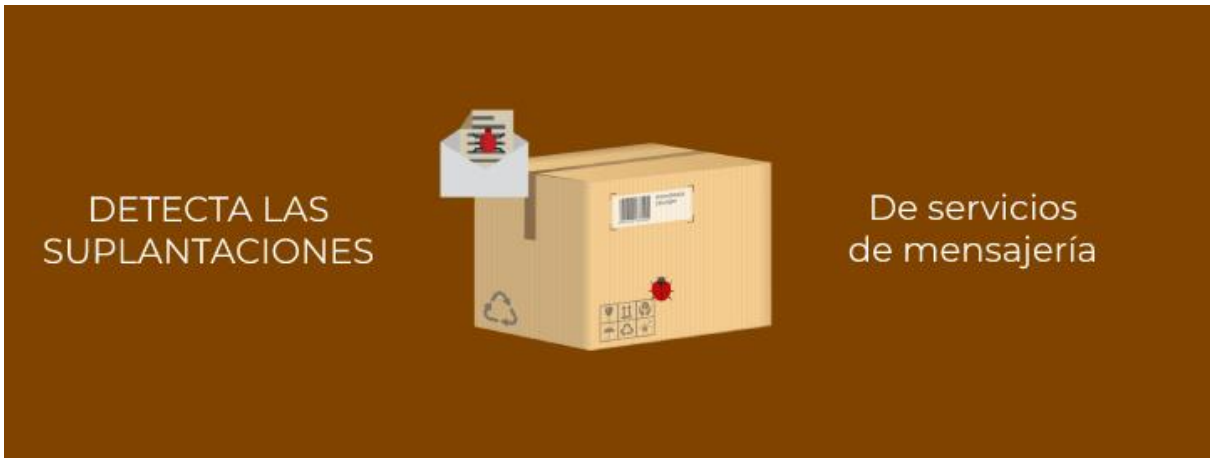
En Mac tenemos la función **FileVault**. Podemos encontrarlo en '**Preferencias del sistema**' > '**Seguridad y privacidad**', en la pestaña '**FileVault**'.



Como siempre decimos, las nuevas tecnologías ofrecen muchas posibilidades, y estando informados, podemos tener la configuración más segura de nuestros dispositivos para nuestra protección y la de nuestros seres queridos. Además, cuentas con la Línea de Ayuda en Ciberseguridad de INCIBE, 017, gratuita y confidencial, para consultar tus dudas y problemas siempre que lo necesites. Tambieén por WhatsApp 900 116 117 o Telegram @INCIBE017.

Publicado el
29/03/2023

Cómo detectar mensajes fraudulentos que suplantan a servicios de mensajería



En los últimos años, muchas tiendas y empresas han optado por vender sus productos y servicios a través de Internet, informatizando y automatizando este proceso, de forma que cuando se compra algo online el cliente recibe un correo o SMS en el que se le comunican los datos de esta transacción, del mismo modo que le mantiene al tanto del estado de su pedido y la entrega del paquete a través de canales como los SMS.

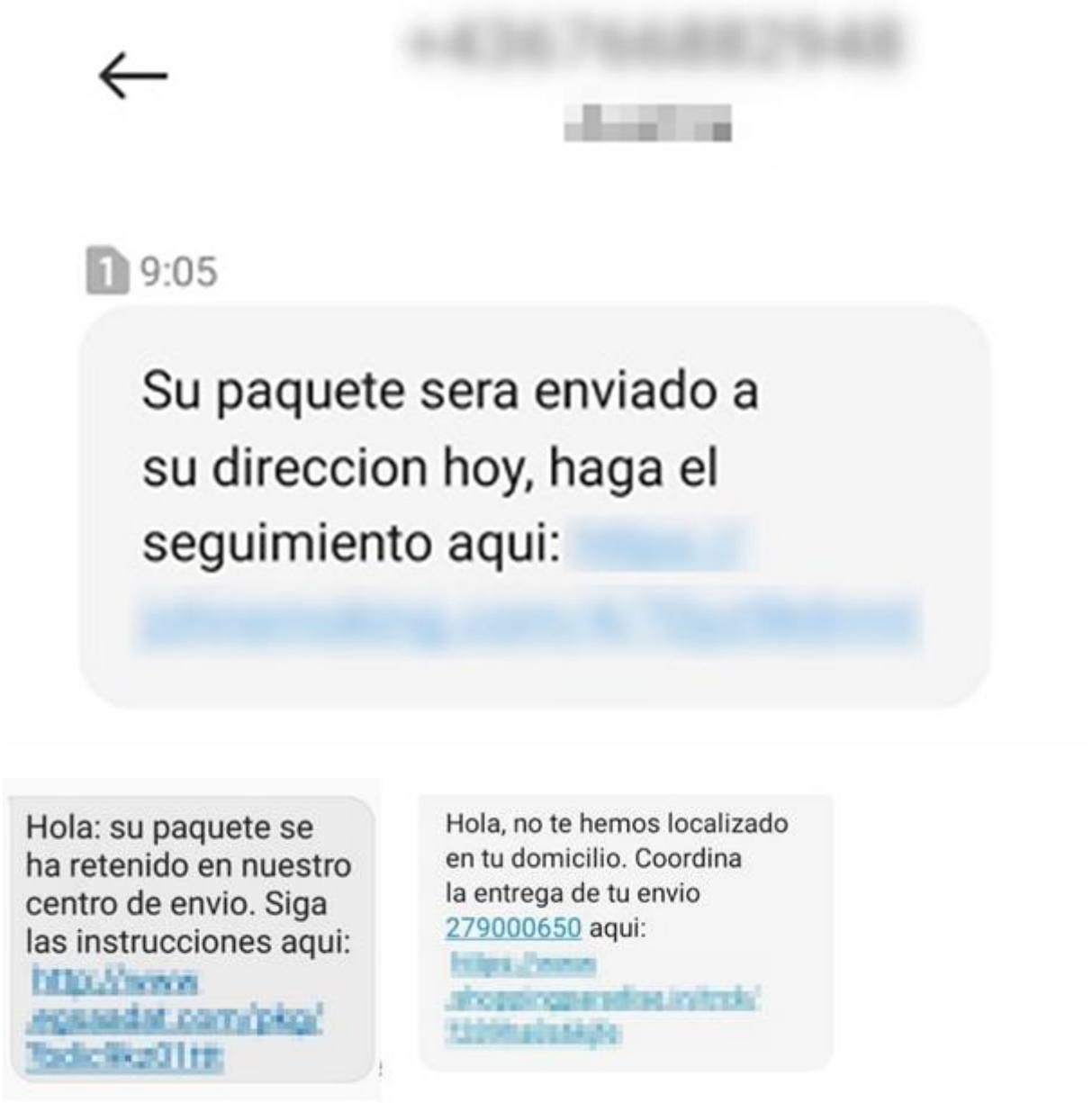
El comercio electrónico, al ganar peso en la Red, se ha convertido en un objetivo para los ciberdelincuentes, creando páginas webs fraudulentas de venta *online*, pero también los servicios complementarios de la venta en Internet, como son las empresas de mensajería y paquetería.

Estas empresas de paquetería son las que contrata una tienda para hacer llegar a sus clientes los pedidos online, por lo que les proporcionan sus datos de contacto, como pueden ser su email o número de teléfono. A través de ellos, envían un número de rastreo del pedido para que el cliente pueda ver dónde se encuentra su paquete y el estado del envío.

Es en este proceso de entrega en el que debemos prestar atención a las notificaciones que nos llegan a nuestras bandejas de correo y de SMS, ya que es aquí donde podemos estar a merced de los ciberdelincuentes si no hacemos una serie de comprobaciones de seguridad.

Los ciberdelincuentes están aprovechando el auge de las compras online para enviar mensajes fraudulentos a los usuarios de manera indiscriminada, suplantando a empresas de mensajería haciendo referencia a algún tipo de problema, como el envío de su paquete o la entrega de este, pidiéndoles que se descarguen una aplicación, un archivo o cliquen en un enlace para confirmar algunos datos.

A continuación, mostraremos ejemplos reales de SMS y webs a las que te redireccionan los enlaces de correos o mensajes de texto maliciosos enviados por los ciberdelincuentes, en los que suplantan a una entidad de las comentadas anteriormente.



En la siguiente imagen se mostrará un ejemplo de una web clonada por un ciberdelincuente, es decir, una web imitando a la página real de un servicio de mensajería y reparto.

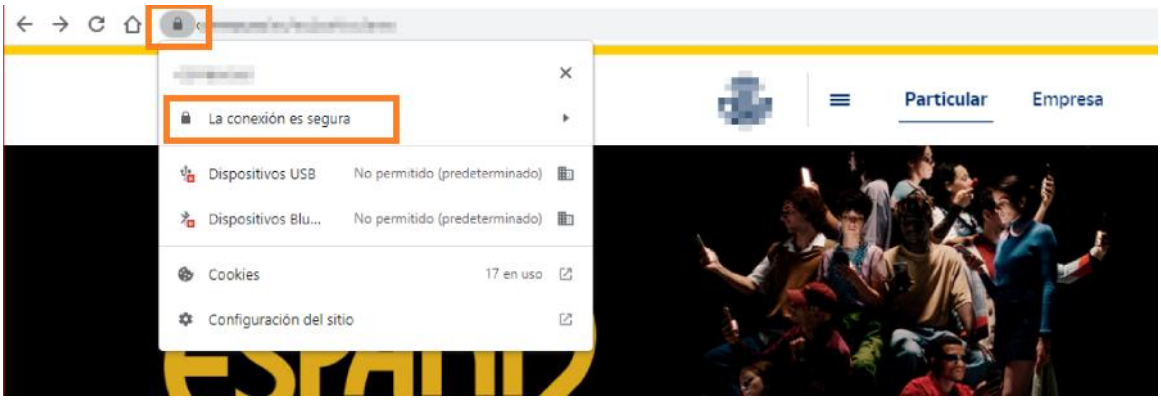
¿Por qué recomendamos hacer comprobaciones de seguridad?

Actualmente, los ciberdelincuentes están explotando unas técnicas de fraude conocidas como *smishing* y *phishing*, por las cuales utilizan los SMS y correos electrónicos para obtener información sobre sus víctimas, ya sean datos personales, bancarios, etc., los cuales utilizan para cargar importes de dinero en dichas cuentas o extorsionar a las víctimas con exponer sus datos a cambio de un beneficio económico. También pueden utilizar dicha información para suplantar la identidad de la víctima y utilizarla para fines fraudulentos.

Pero, ¿es la única forma que tienen de comprometer nuestra seguridad? La respuesta es no. En muchas ocasiones, al hacer clic en los enlaces de estos correos y mensajes de texto maliciosos, descargamos archivos o virus en nuestros dispositivos, por lo que debemos revisar bien los enlaces y documentos adjuntos que recibimos antes de realizar ninguna acción sobre ellos.

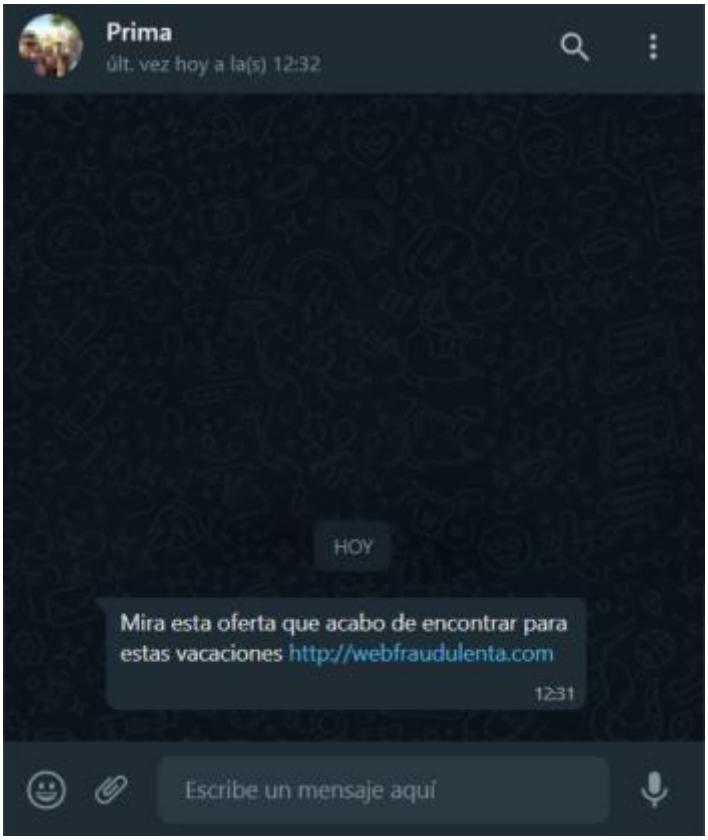
A continuación, explicaremos qué **comprobaciones** debemos hacer cuando recibamos un SMS o correo de una empresa de mensajería y reparto para comprobar si realmente es quien dice ser o se trata de un mensaje fraudulento, cuyo objetivo es engañarnos para que accedamos a un enlace malicioso.

1. Siempre que tengas dudas de la veracidad de un correo o SMS, puedes contactar con la empresa de reparto. Busca en tu navegador la web oficial de dicha empresa y llama al teléfono o correo que proporcionen. Además, muchos de estos servicios han creado un área de respuesta a incidentes para atender casos de posibles fraudes que utilicen su marca e imagen, por lo cual puedes contar con ellos para que te informen sobre algún caso particular. Para comprobar que es la web oficial del servicio de reparto, revisa que la URL comience por **https://.** Además, debes mirar si el navegador muestra un **símbolo de un candado**. Al hacer clic en él, mostrará qué **tipo de certificado SSL** tiene instalada la web.

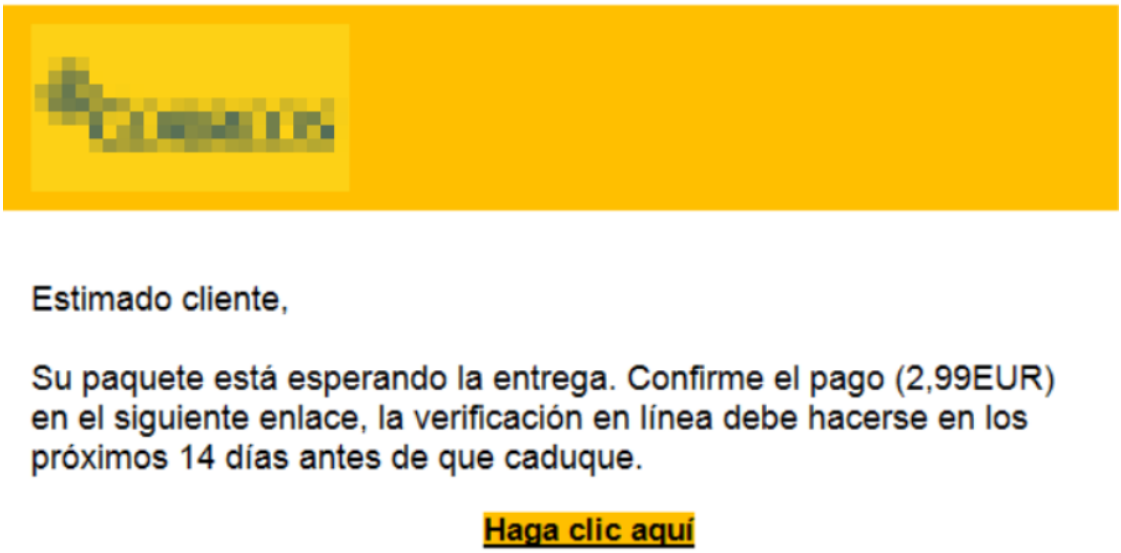


2. Hay gran variedad de virus destinados a infectar nuestros dispositivos, que utilizan como pretexto el seguimiento de un paquete, especialmente para móviles. Generalmente, intentan engañarnos para que instalemos programas maliciosos que suelen venir **ocultos** en una "aplicación" de una empresa de reparto para el rastreo de un paquete. Por norma general, antes de descargar la aplicación que te ofrecen a través de un enlace o mensaje, búscala en las tiendas oficiales de tu dispositivo, asegurándote de que es la oficial de la empresa. **¡Nunca descargues una app a través de un QR o enlace que te proporcionen en un SMS o email!**

3. Si recibes un enlace o archivo de una persona conocida, pero no habías pedido que te lo enviara y la explicación que te proporciona no es con el vocabulario que comúnmente utiliza contigo, **confirma con esa persona que te lo ha enviado voluntariamente, es decir, que te ha enviado conscientemente dicho enlace y qué contiene o qué vas a encontrar en él**. Además, puedes colocar el cursor del ratón sobre el link, sin hacer clic, para saber adónde te va a redirigir. En el caso de un móvil, puedes saber la dirección de destino del enlace presionando varios segundos sobre él.



4. ¿Te exigen con urgencia que compruebes algo en el SMS o correo? ¡Desconfía de las prisas! Es una de las estrategias utilizadas para captar la atención de las posibles víctimas.



Estimado cliente,

Su paquete está esperando la entrega. Confirme el pago (2,99EUR) en el siguiente enlace, la verificación en línea debe hacerse en los próximos 14 días antes de que caduque.

Haga clic aquí

¿Qué pueden provocar en nuestros dispositivos estos fraudes si somos víctimas de ellos?

Si descargamos un programa malicioso, no solo puede dañar o deshabilitar funciones de nuestros dispositivos, sino que también pueden monitorizar todas las acciones que se realicen desde ellos, es decir, acceder a información almacenada como fotos y vídeos, conectarse a Internet, ver el contenido de los SMS, etc., pudiéndose utilizar toda esta información en nuestra contra, como, por ejemplo, suplantación de identidad en redes sociales y otras plataformas, extorsión, etc.

Recomendaciones que te pueden ayudar a estar más protegido frente a estos programas maliciosos que puedes recibir a través de mensajes maliciosos:

- Mantén tus dispositivos actualizados y protegidos con antivirus, ellos son la primera barrera defensiva contra los programas maliciosos.
- Inhabilita la opción "Instalación de aplicaciones de orígenes desconocidos" en la configuración de tus dispositivos para no descargar aplicaciones no deseadas de fuentes no oficiales o desconocidas.
- No descargues aplicaciones o programas a través de enlaces recibidos, búscalos en las tiendas y webs oficiales.
- Realiza copias de seguridad de tus dispositivos frecuentemente para no llevarte disgustos y almacena dichas copias en lugares externos a tu dispositivo, como discos externos o en un servicio en la nube.
- No facilites tus datos a páginas que pienses que son sospechosas o que desconoces su legitimidad.
- No abras archivos adjuntos ni ejecutables sin confirmar la entidad del emisor del mensaje.
- Si te solicitan un pago a través de SMS o correo, desconfía y consulta directamente a las fuentes implicadas a través de otras vías, asegurándote de que son las oficiales.

Google Dorks te ayuda a encontrar información sobre ti en la Red

En la actualidad todo el mundo utilizamos Internet como solución a diferentes dudas que se nos plantean en nuestro día a día y lo primero que solemos hacer es abrir una pestaña para utilizar "google.com". Sin embargo, ¿alguna vez has pensado qué información hay sobre ti en Internet? En este artículo te mostraremos cómo puedes utilizar este recurso llamado "Google Dorks" para encontrarla y sepas qué hacer en caso de que no desees que aparezca en los resultados.

¿Qué es Google Dorking?

Google Dorks o *Dorking*, también conocido como Google *Hacking* es una técnica que consiste en aplicar la búsqueda avanzada de Google para conseguir encontrar en Internet información concreta a base de ir filtrando los resultados con operadores conocidos como *Dorks*, que son símbolos que especifican una condición. Por ejemplo, si ponemos en nuestro texto de búsqueda las dobles comillas ("texto"), buscará información que coincida exactamente con el texto. Es decir, si buscamos "OSI", nos devolverá el contenido que concuerde exactamente con ese término. A lo largo de este artículo te enseñaremos cómo te puede ser útil.

¿Qué puedes encontrar con Google Dorks?

Dependiendo de los parámetros utilizados para la búsqueda, los resultados cambiarán, pero podría ser posible identificar información de todo tipo:

- Credenciales: usuarios y contraseñas de tus cuentas.
- Contenido audiovisual: fotos y vídeos.
- URLs privadas.
- Documentación sensible: DNI, números de teléfono, otros carnets.
- Información bancaria: números de cuenta o tarjetas.
- Correos electrónicos.
- Acceso a cámaras de seguridad.
- Etc.

¿Es legal usar Google Dorks?

Es importante que antes de lanzarte a utilizar Google Dorks, tengas claro que la información que quieres obtener o estás buscando no debes utilizarla para perjudicar a otras personas o que el objetivo de obtener dicha información sea para fines poco éticos.

Teniendo claro el párrafo anterior, la respuesta a la pregunta: ¿es legal usar Google Dorks? La respuesta es sí, ya que toda la información que puedes encontrar cuando realizas las búsquedas, es información pública, es decir, está expuesta y publicada en Internet bien sea consciente o inconscientemente por ti mismo o incluso por terceras partes.

En los siguientes apartados te enseñaremos cómo puedes utilizar esta herramienta para encontrar información sobre ti, para que tomes las medidas que consideres necesarias en cada caso.

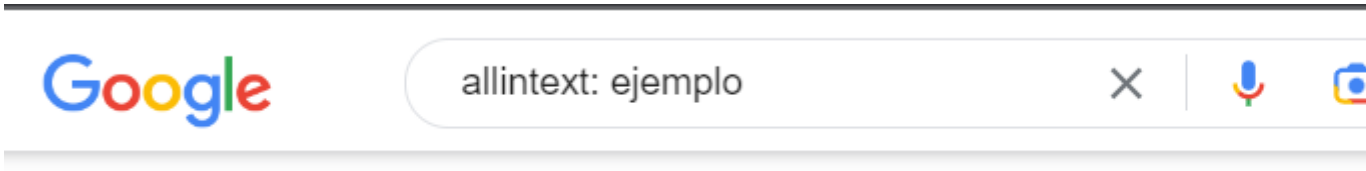
¿Cómo utilizar Google Dorks?

Primero necesitas conocer los comandos básicos de las búsquedas avanzadas. Se llaman **operadores** y son símbolos o palabras específicas con las que puedes encontrar algo en concreto que busques.

Por ejemplo, si quieres comprobar si tu nombre aparece en páginas web, puedes introducir en la barra de navegación de tu buscador: "Tu nombre y apellidos" entre comillas. Del mismo modo, puedes realizar búsquedas entrecomillando lo que quieras encontrar: "número de dni", "dirección de casa", "teléfono", "email", "matrícula del coche", etc.

Por otro lado, si te gustaría saber si están expuestas tus credenciales de acceso a algún servicio online que utilices, es decir, si están publicadas en alguna web accesibles para todo el mundo debido algún hakeo o robo de datos, debes utilizar el operador **inurl** e **intext** tal que así: **inurl**: [URL de la web] **AND intext**: [contraseña]

También, si quieres buscar palabras en concreto que contengan una página web, puedes usar el operador **allintext**: (palabra deseada). Ejemplo: **allintext**: noticias coronavirus.



Otra utilidad interesante de esta herramienta es que puedes hacer búsquedas para encontrar documentos e información específica. Por ejemplo, puedes buscar si en una página web está expuesto tu currículum vitae, con el comando **site**: [página web] y entre comillas los datos que te ayuden a localizarlo: "teléfono" "correo" "dirección", etc. Por último, buscamos el documento en sí con **intitle**: "currículum vitae". Ej. **site**:paginaweb.com "teléfono" "dirección" "correo electrónico" **intitle**: curriculum vitae.

Hay otros muchos operadores que puedes utilizar, en la página de soporte de Google encontrarás más información: https://support.google.com/websearch/answer/2466433

¿Qué hago si mi información ha sido expuesta?

En caso de que hayas encontrado en la red datos personales o privados, puedes seguir una serie de pautas:

- Si consideras que una información sobre ti no debería ser visible y accesible para cualquiera, solicita su eliminación mediante Google Search Console. Podrás solicitar la retirada de información como la siguiente:
  - Imágenes íntimas no consentidas.
  - Información personal que permita identificarte o ponga en riesgo tus datos bancarios.

- Además, si encuentras públicas tus claves, cámbialas por contraseñas únicas y fuertes para cada cuenta, incluyendo en estas mayúsculas y minúsculas, números y caracteres especiales. Esto limitará el riesgo de que un ciberdelincuente o una persona malintencionada acceda a tus cuentas con la información que haya conseguido usando estas búsquedas avanzadas de Google. También se recomienda el uso de la doble autenticación para acceder a tus cuentas y así dificultar el robo de estas. Es complicado recordar contraseñas robustas, por lo que usar un gestor de contraseñas que te ayude a almacenarlas y crearlas es una buena forma de mantenerte seguro/a y hacer esta tarea algo más fácil.

- Finalmente, protege tus dispositivos con un antivirus actualizado y ejecuta análisis regulares para evitar vulnerabilidades de seguridad en tus dispositivos y prevenir que tu seguridad y datos se vean comprometidos.

En definitiva, ser conscientes de la información sobre nosotros que hay en Internet nos facilita poner los medios necesarios para proteger nuestra privacidad y conservar nuestra seguridad. En caso de no saber cómo actuar o tener alguna duda sobre las buenas prácticas en temática de ciberseguridad, contacta con nosotros a través de Línea de Ayuda en Ciberseguridad de INCIBE, llamando al teléfono gratuito 017, contactando a través de WhatsApp (900 116 117) o Telegram (@INCIBE017).