



Una de las situaciones más riesgosas, y lamentablemente, más comunes, es la violación de datos causada por una filtración de seguridad de algún hacker o malware. Aquí te contaremos qué hacer si has detectado alguna filtración de datos en tus cuentas o equipos.

¿Qué es una filtración de datos?

Las filtraciones de datos consisten en el robo o acceso a datos por parte de personas malintencionadas quienes pueden ser otros usuarios o hackers. Básicamente se trata de alguien ajeno, sin autorización ni buenas intenciones, obtiene datos de valor para ti como información personal, bancaria, privada, de tu empresa, etc.

Existen diferentes casos de filtración de datos que van desde los más simples como tu nombre o dirección IP, hasta filtraciones de fotos íntimas de usuarios y famosos o incluso [casos de filtraciones de datos masivas](#) para empresas lo cual supuso un impacto económico y de seguridad brutal.

Pasos a seguir ante una filtración de datos

### 1. Comprobar si fuiste víctima de una filtración de datos

Antes de tomar acciones, es necesario comprobar si realmente fuimos víctima de una filtración de datos, así como la forma en la que fuimos víctimas.

Te recomendamos buscar una [guía sobre cómo verificar si fuiste víctima de una filtración de datos](#) para así comprobar si realmente pasó dicha situación. Además, existen algunas formas de develar el origen de dicha filtración para saber si fue un hackeo, un enlace fraudulento, un malware o alguna otra artimaña.

- Aislar a tu equipo

Una vez que identificamos que realmente fuimos víctima de un ataque y se han filtrado nuestros datos, es momento de aislar nuestro equipo. Lo recomendable es cerrar todas



nuestras cuentas como la de correo o redes sociales. Después, debemos de desconectar nuestro equipo de internet para evitar una mayor filtración.

Tras aislar tu equipo, el siguiente paso es detectar cómo es que se ha dado la filtración para proceder a solucionarla. Por ejemplo, si fue por medio de una página web, esto es mucho más fácil de solucionar que un hackeo o un programa dañino.

- Limpiar todo tu equipo

Eliminada la amenaza, recomendamos realizar una desinfección completa de tu equipo, ya que es probable que este haya quedado vulnerado. Esto incluye correr programas para detectar algún tipo de programa malicioso que no hayamos visto al cerrar la brecha de seguridad.

También, de ser necesario, debemos de actualizar el sistema para instalar los parches de seguridad correspondientes que puedan bloquear algún tipo de vulnerabilidad. Incluso algunos expertos en ciberseguridad recomiendan formatear todo tu equipo para así garantizar que este quede 100% limpio, lo cual puede ser necesario si la fuga de datos fue muy grave.

- Proteger a tu equipo

Una vez que quede limpio y libre de filtraciones es necesario proteger nuestro equipo para evitar una reincidencia. Para ello debemos de instalar software como un antivirus, por ejemplo, y una VPN los cuales nos ayudarán a que no se cuelen ni hackers ni programas maliciosos.

La VPN, por ejemplo, ofrece una gran ventaja, ya que permite crear un escudo entre internet y tu ordenador por lo que te recomendamos que [compruebes el software VPN gratuito para conocer el período de prueba](#) para así conocer todos los beneficios que te ofrece protegiendo tus datos y tu seguridad.



- Tomar otras medidas

Por último, será necesario adoptar algunas medidas para prevenir que esto vuelva pasar como tener un mejor control de quien usa nuestro equipo. De igual forma, colocarle una contraseña puede ser una buena forma de evitar una fuga de datos por parte de un usuario que haya ingresado a nuestra PC.

También te recomendamos que seas mucho más cuidadoso a la hora de descargar archivos y de usar páginas web. Además, será de gran utilidad aprender a detectar posibles enlaces fraudulentos y otras técnicas usadas por los hackers para el robo de información.

### Los riesgos de una filtración de datos

Aunque muchos podrían pensar que no hay riesgos en la filtración de datos, en realidad esto no es así. Una filtración de datos puede ser realmente dañina, sobre todo cuando se filtra información muy delicada tanto para tu seguridad como tu privacidad.

Por ejemplo, la filtración de secretos industriales puede ser, sin lugar a dudas, un golpe muy duro para una empresa lo cual puede llevarla incluso a quebrar. Por otro lado, una filtración de tu información bancaria o de información íntima no solo puede provocar momentos difíciles y vergonzosos, también puede llevarte a perder dinero, por ejemplo, por un robo.