Haz copias de seguridad y cifra tus datos

Por qué hacer copias de seguridad

Las pérdidas de información suelen presentarse de manera inesperada y pueden provocar daños irreparables. Las causas por las que podemos perder nuestros archivos más preciados pueden ser de diferente índole:

- **Avería total o parcial de los discos duros**, del ordenador o externos. Aunque en ocasiones aparecen síntomas que nos pueden alertar, la mayoría de las veces el fallo es repentino y sin posibilidades de recuperación.
- **La gran variedad de dispositivos móviles que utilizamos** (portátil, tableta, smartphone, etc.) hace que aumente la probabilidad de perderlos o que nos lo roben, con la consiguiente pérdida de información.
- **El deterioro físico** provocado por el tiempo y el uso afecta también a soportes como los CDs y DVDs.
- **El borrado accidental** es otro modo de perder información. No todo podremos rescatarlo de la papelera de reciclaje. Por ejemplo, no podremos recuperar ficheros sobrescritos en el ordenador o archivos eliminados en móviles como Android.

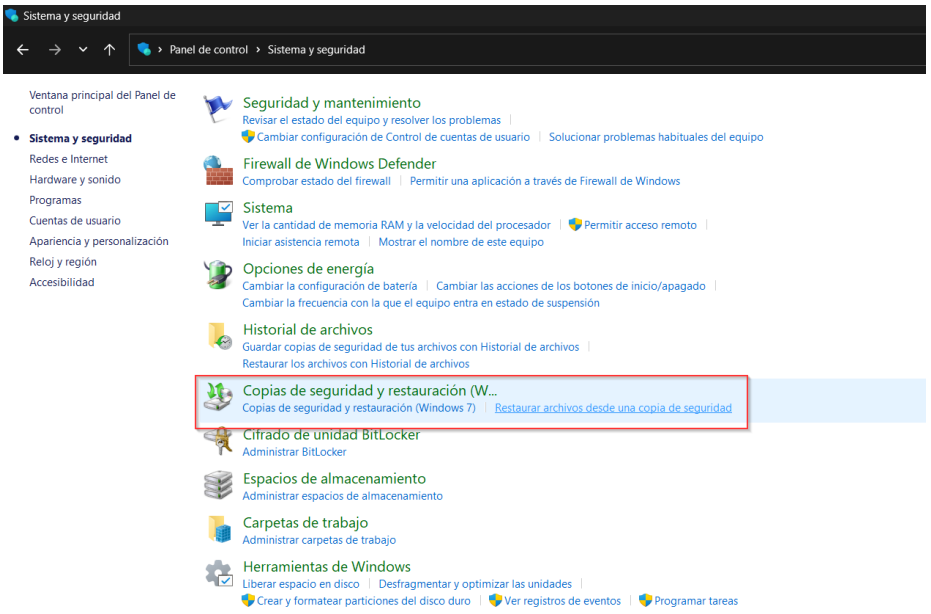
- **Algunos tipos de virus** pueden provocar la destrucción o borrado de los archivos y quedar irrecuperables. Un ejemplo de esto es el famoso virus que suplanta al servicio de Correos y Telégrafos (***Postal service scam***).

Cómo hacer las copias de seguridad

Las copias de seguridad son "segundas copias" de nuestros archivos que deben mantenerse siempre en dispositivos diferentes al original. Veamos de cuántas maneras podemos realizarlas.

1. **En discos externos conectados mediante USB**. Es el modo más recomendable para realizar las copias de seguridad. La gran capacidad de los dispositivos actuales permite guardar todos nuestros archivos valiosos.
   Podemos realizar copias de dos formas diferentes:
   - **Manual.** Seremos nosotros, los que de manera proactiva copiemos aquellos archivos que nos parezcan más importantes salvaguardar en otro soporte. Para recuperar una copia, simplemente conectaremos de nuevo el disco duro, USB, DVD, etc. o el soporte que hayamos utilizado para realizar las copias a nuestro ordenador o dispositivo que corresponda y rescataremos los archivos que necesitemos.
   - **Automática.** Es posible programar la realización automática de copias de seguridad de manera periódica, para que no tengamos que estar pendientes nosotros de esta tarea, una opción muy práctica y cómoda para la mayoría de nosotros. Tras realizar una primera copia de seguridad completa, la siguiente que hagamos podemos programarla para que copie únicamente aquellos archivos que hayan sido modificados, lo que supone un ahorro importante de espacio de almacenamiento.

1. Si somos usuarios de Windows, para realizar esta tarea podemos hacer uso de la funcionalidad que viene integrada con el sistema operativo Windows "Copias de seguridad y restauración".



2. En los equipos MAC, se puede utilizar "Time Machine" **Guía**
3. En dispositivos Android a través de una copia de seguridad con una cuenta de Google **Guía**
4. Para copias de seguridad en dispositivos iOS se puede hacer uso del servicio iCloud y también iTunes. **Guía**

2. **En la nube.** Existen servicios que nos ofrecen espacio en Internet para almacenar archivos.

   DropBox: **Guía**

   Google Drive: **Guía**

   One Drive: **Guía**

Son algunos de los más conocidos, pero existen muchos más.

3. **DVD o Blu-ray.** Si deseamos realizar copias en soportes físicos, podremos escoger como formato de almacenamiento alguno de estos dispositivos. Eso sí, teniendo en cuenta si estos discos son compatibles con nuestro grabador, pues no todos admiten los formatos más recientes. Los programas diseñados para realizar copias de seguridad pueden utilizar discos de este tipo como destino de grabación. Recurrir a discos "regrabables", puede ser una buena elección, ya que nos evita acumular un gran número de ellos, especialmente si no hemos ocupado el espacio total de almacenamiento.

Cifrado de Datos

Cómo cifrar tus archivos y carpetas más importantes

Solemos trabajar con información importante, privada y confidencial que no queremos que llegue a manos de cualquier persona y que pueda usarla en nuestra contra. Información personal, información confidencial de trabajo, estudios, investigaciones… Hay documentos que no queremos compartir o poner en peligro. Además, no siempre trabajamos en un ordenador propio, sino que compartimos espacio u oficina con otras personas y queremos que nuestros documentos no estén al alcance de cualquiera. En

este caso, lo mejor es encriptar los archivos que utilizamos para que nadie pueda acceder a ellos sin nuestro permiso.

Antes de saber cómo podemos encriptar todos los programas o cifrar nuestros archivos, conviene que tengamos en cuenta algunos aspectos importantes a la hora de utilizar este método o si merece la pena o qué tipo de contenidos podemos cifrar o encriptar.

Qué tener en cuenta

Como hemos dicho en el párrafo anterior, en los próximos párrafos te explicaremos cómo podemos encriptar o cifrar programas y qué herramientas debemos usar pero antes debes tener claro qué es encriptar o cifrar y también debes tener claro que hay diferentes tipos de cifrado que podemos y con diferencias entre sí en sus características dependiendo lo que necesites.

¿Qué es encriptar o cifrar?

Según la Real Academia Española, **encriptar o cifrar es** "transcribir con guarismos, letras o símbolos, de acuerdo a una clave, un mensaje o texto cuyo contenido se quiere **proteger**. Es decir, proteger nuestros archivos o carpetas con documentos para que nadie acceda sin nuestro permiso y pueda ver lo que hay. Cifrar consiste en utilizar un algoritmo de cifrado y con una clave o contraseña que alteran el origen de los datos de un documento o carpeta de modo que no puedan ser leídos por un tercero en caso de que este llegue a ellos.

En el caso de encriptar documentos en un ordenador, solemos utilizar casi siempre el cifrado por bloques de tipo **AES** (Advanced Encryption Standard) Se trata de un tipo de

cifrado simétrico que utiliza un algoritmo en el que los archivos se cifran con una contraseña y se descifran con esta misma clave. Utilizando una contraseña podrás devolver los datos a su estado original y ver el contenido. Si tienes un disco duro cifrado o un pendrive cifrado, por ejemplo, cuando guardes o copies un archivo a ese disco, se cifra automáticamente y se descifra o desencripta en el momento en el que lo sacas del disco que está cifrado.

El cifrado de datos es algo habitual en los formatos digitales por los que viaja la información. Independientemente de si se trata de usuarios particulares e individuales o grandes compañías, la mayoría de información con contenidos delicados suele viajar encriptada. Nuestros chats en aplicaciones de mensajería van cifrados de extremo a extremo, solo los usuarios pueden acceder al contenido de las conversaciones. De igual manera, aunque con algoritmos más avanzados, las compañías que albergan datos personales, bancarios, etc. en sus servidores (tiendas online, banca electrónica, almacenamiento en la nube, etc.) también almacenan todos los datos con elevados niveles de seguridad para que no puedan ser rastreados y extraídos.

La información encriptada mediante un algoritmo necesita de una clave especial para poder descomprimir la información (desencriptarla), esta clave puede ir acompañando al bloque de información para ser utilizada, o enviada directamente al servidor del destinatario.

Tipos de cifrado

Aunque nos ha quedado claro qué es cifrar o encriptar programas o documentos, no solo existe un método y hay varios tipos de cifrado diferentes que podemos tener en cuenta y que tienen diferencias entre sí, dependiendo del que queramos utilizar. Existen diferentes tipos de cifrado según sus claves:

- **Cifrado simétrico:** Es el que utiliza la misma clave para cifrar y descifrar el mensaje. Por lo tanto, deben conocerla tanto el emisor como el receptor.
- **Cifrado asimétrico:** Se basa en el uso de dos claves, una pública y otra privada. La clave pública se puede compartir con aquellas personas a las que vamos a enviar un archivo cifrado, mientras que la clave privada es la que no se debe desvelar nunca.

La principal ventaja del cifrado simétrico es que es mucho más rápido, por lo que, si necesitamos cifrar gran cantidad de información, el uso de este tipo de cifrado será mucho más sencillo. En lo que a seguridad se refiere el cifrado asimétrico permite enviar, de forma segura, claves públicas a terceros, mientras que la clave privada siempre permanece con el usuario. Por su parte, el cifrado simétrico no es tan seguro ya que el hecho de facilitar la misma clave supone un riesgo. Ahora bien, dentro de cada uno de estos tipos de cifrado, se puede hacer otra clasificación en función del algoritmo que se utilice, en el caso del cifrado simétrico el más popular y utilizado es AES, mientras que en el asimétrico son RSA y DSA.

- **Cifrado AES**

  El Estándar de Cifrado Avanzado (Advanced Encryption Standard, o AES), lo utilizan los gobiernos y las organizaciones de seguridad, así como las empresas privadas para las comunicaciones clasificadas. AES utiliza un cifrado de clave simétrico. Alguien en el extremo receptor de los datos necesitará una clave para decodificarlos.

  AES se diferencia de otros tipos de cifrado en que cifra los datos en un solo bloque, en lugar de como bits de datos individuales. Los tamaños de bloque determinan el nombre de cada tipo de datos cifrados AES:

  AES-128 cifra bloques de un tamaño de 128 bits.

  AES-192 cifra bloques de un tamaño de 192 bits.

  AES-256 cifra bloques de un tamaño de 256 bits.

  Además de tener diferentes tamaños de bloque, cada método de cifrado tiene un número diferente de rondas. Estas rondas son los procesos de convertir un

fragmento de datos tipo texto en datos cifrados o texto cifrado. AES-128, por ejemplo, usa 10 rondas y AES-256 usa 14 rondas.

La mayoría de las herramientas de datos disponibles en el mercado hoy en día utilizan cifrado AES. Incluso aquellos que te permiten utilizar otros métodos con sus programas recomiendan el estándar AES. Funciona en muchas aplicaciones y sigue siendo el método de cifrado más seguro y aceptado por su precio. De hecho, probablemente lo estés usando sin siquiera saberlo.

Programas para cifrar documentos

Sea cual sea el documento que estás utilizando, hay **programas encargados de cifrarlos** para que estén protegidos y que tu información siga **siendo confidencial.** Esto es útil si tienes datos privados que no quieres que nadie vea o si vas a subirlos a una solución de almacenamiento en la nube y quieres mejorar aún más la privacidad. Sea como sea, existen programas para encriptar documentos por los que no tendrás que pagar nada y que son compatibles con todo tipo de sistemas operativos.

Estos son algunos de los programas más usados para encriptar en Android, en iOS o en Windows.

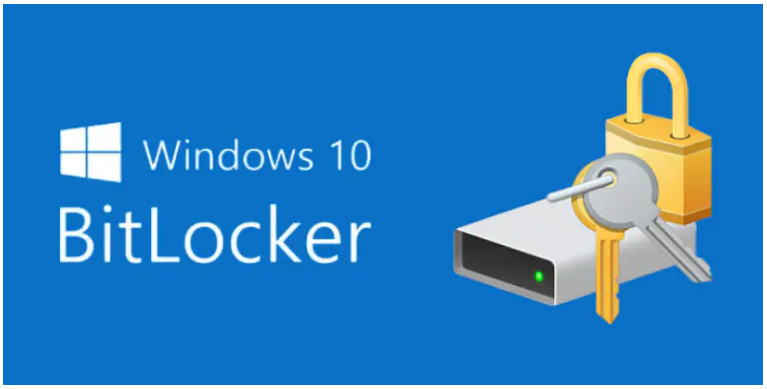
Cryptomator

Una de las mejores herramientas gratuitas para cifrar o encriptar es Cryptomator, un software sencillo, de código abierto, que no requiere ningún tipo de registro y es compatible con la mayoría de sistemas operativos como Windows, macOS, Linux o

Android o iOS para teléfonos móviles. Lo que nos permite Cryptomator es crear una especie de gran carpeta cifrada con protocolo AES, como si se tratase de una caja fuerte, y a la que nadie puede acceder sin nuestro permiso. En esta "caja" podrás meter todo tipo de archivos que no quieres que nadie los vea sin el código correcto de desbloqueo.
La ventaja de Cryptomator es que no sólo te permite crear una carpeta protegida en tu ordenado de forma local, sino que también puedes hacerlo en Dropbox o en Google Drive y tendrás sincronizados los documentos guardados en el almacenamiento en la nube sin que nadie pueda leerlos sin tu permiso. Otra de las principales ventajas es que podrás descargarlo para tu teléfono móvil con las aplicaciones de iOS y Android, aunque en este caso tendrás que pagar 9,99.

Descarga Cryptomator para Windows | Descarga la aplicación de Cryptomator para Android | Descarga para iOS

Bitlocker



BitLocker es la herramienta que ofrece Microsoft si tienes una versión de Windows de tipo Profesional o Enterprise y te permite cifrar cualquier tipo de archivo o contenido:

del disco duro interno de tu ordenador o de discos de arranque, pero también cifrar un USB que conectes o de discos duros externos que quieras o necesites utilizar. En este caso, BitLocker utiliza XTS-AES con una clave de 128 bits para discos internos o de datos o un algoritmo AES-CBC con clave de 128 bits para discos externos. No obstante, esto se puede cambiar para que sea AES-XTS 256 bits, aunque debes tener en cuenta que en los primeros Windows 10 y sistemas operativos anteriores (como Windows 8.1, Windows 8 o Windows 7) no será compatible con este tipo de cifrado.

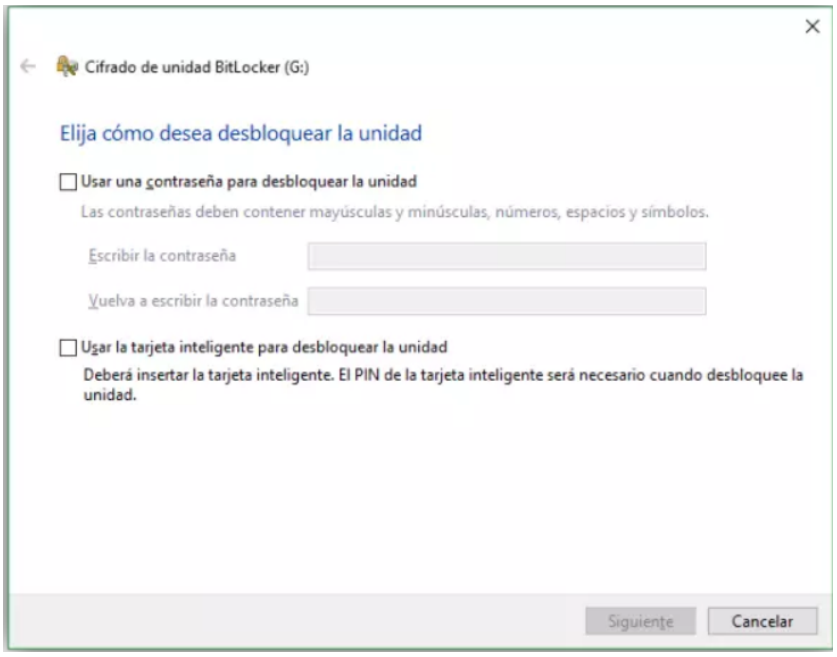
Si tienes una versión de Windows 10 (que no sea la edición Home) puedes activar el cifrado del dispositivo fácilmente, según puedes leer en la propia página web de Microsoft. Simplemente inicia sesión en Windows con la cuenta de Administrador, ve al botón de Inicio y sigue estos pasos:

- ✔ Abre Inicio
- ✔ Ve a Configuración
- ✔ Accede a Actualización y seguridad
- ✔ Ve a Cifrado de dispositivos
- ✔ Selecciona la opción **"Activar"**

También podrás activar el cifrado de dispositivo de BitLocker estándar:

Inicia sesión con cuenta de administrador

- ✔ Ve al botón de Inicio
- ✔ Busca Sistema Windows
- ✔ Elige Panel de control
- ✔ Selecciona Sistema y seguridad
- ✔ Elige Cifrado de unidad BitLocker
- ✔ Selecciona Administrar BitLocker
- ✔ Activa BitLocker
- ✔ Sigue las instrucciones que te indica el programa



AES Crypt

AES Crypt es un software de encriptación que puedes usar en macOS, Linux o Windows y que es **totalmente gratuito** y de código abierto. Una vez que descargas la herramienta en tu ordenador, **se integra con el menú** así que siempre la tendrás a mano para encriptar cualquier archivo sin ningún tipo de complicación. Es decir, una vez que descargas e instalas este software y pulsas sobre el botón derecho de cualquier archivo, verás que aparece entre las opciones y que puedes añadir la contraseña. Es muy sencillo de manejar y creará un nuevo archivo, cifrado con la clave que has elegido, que podrás usar para lo que necesites.

Para leer archivos con AES Crypt el funcionamiento es el mismo que para cifrar o encriptar: haz clic derecho sobre el documento en cuestión, se abrirá el menú con opciones y podrás **elegir este software.** Una vez que lo elijas, introduce la contraseña que tenía el archivo y estará listo para abrirlo, leerlo o editarlo como quieras. El archivo con el código fuente está disponible para todo aquel desarrollador que le interese trabajar con esta aplicación. Aunque la descarga de la misma está disponible para **Windows** en versiones de 32 y 64 Bits, para **Android, iOS y macOS** y también las versiones desarrolladas para **Linux** y en **Python**.