Guía de Cifrado

Preguntas y respuestas sobre el cifrado de la información personal

La guía para aprender a cifrar tu información

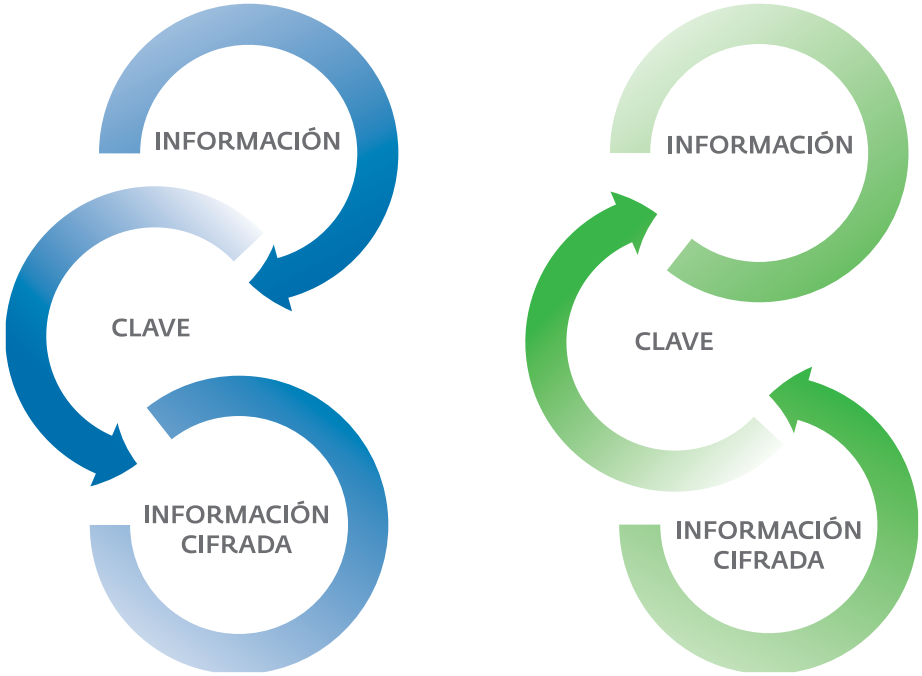
¿Qué es lo que estamos cuidando?

A través del cifrado cuidamos de fotos, videos, mensajes de texto, conversaciones de chat, documentos, contactos y más. Cada vez es **mayor la cantidad de información** que guardamos en nuestros dispositivos, y también es cada vez es **más sensible**. Por ello, se vuelve una tarea indispensable **protegerla** ante los diversos riesgos que existen.

Actualmente, las amenazas para la información van desde códigos maliciosos, o la explotación de vulnerabilidades, hasta el robo de dispositivos móviles. Además, a raíz de la discusión sobre la **privacidad de las comunicaciones** que se está generando, el concepto de cifrado de datos **se popularizó como una forma de mantener la información segura**.

Manejar adecuadamente la información es clave a la hora de sufrir algún incidente, y será determinante para evitar ser afectados.

¿En qué consiste el cifrado de datos?



Cuando se cifra la información, los datos se alteran de acuerdo a un patrón establecido por una clave, de tal forma que **solamente puedan ser entendidos por quienes conocen esa clave**.

Así, un mensaje cifrado puede ser enviado de un lugar a otro o almacenado en algún dispositivo. Si alguien accede a ese archivo sin poseer la clave, **no podrá ver la información**.

No obstante, existen ataques para intentar acceder a esos archivos **sin la clave**. La **dificultad** para descifrar la información a partir de un ataque dependerá de la **forma de cifrado, la información y la clave utilizada**.

> **Las técnicas de cifrado se utilizan desde hace mucho tiempo. En la antigua Roma se utilizaba la "Cifra de César", que consistía en remplazar cada letra de un mensaje por otra letra que se encuentre 3 posiciones más adelante en el alfabeto.**

¿Realmente necesito cifrar mis datos?

Como usuarios podríamos pensar que tal vez nuestra información no sea blanco de un atacante, de modo que quizás sea conveniente hacerse las siguientes preguntas:

¿Qué tipo de información almaceno en mi dispositivo?
Información personal, financiera o confidencial. Es interesante pensar qué tanto podría conocer un tercero si accede a la información que guardo en alguno de mis dispositivos.

¿Qué pasa si pierdo mi dispositivo móvil o mi computadora portátil?
Podemos estar seguros que si perdemos o nos roban algún dispositivo realmente nadie podrá acceder a la información que poseemos.

¿Qué ocurre si el dispositivo es infectado con algún código malicioso?
No solamente si se pierde el dispositivo físico la información puede ser robada. Existen otros tipos de amenazas que pueden robar lo que tenemos almacenado.

Entonces, ¿debo cifrar toda mi información?

Cada vez almacenamos más información, por lo que cifrarla toda puede afectar en el rendimiento de nuestro dispositivo. Entonces, deberemos seleccionar los datos a cifrar en función de su relevancia:

- **Fotografías y videos**
- **Información de contactos**
- **Documentos confidenciales**

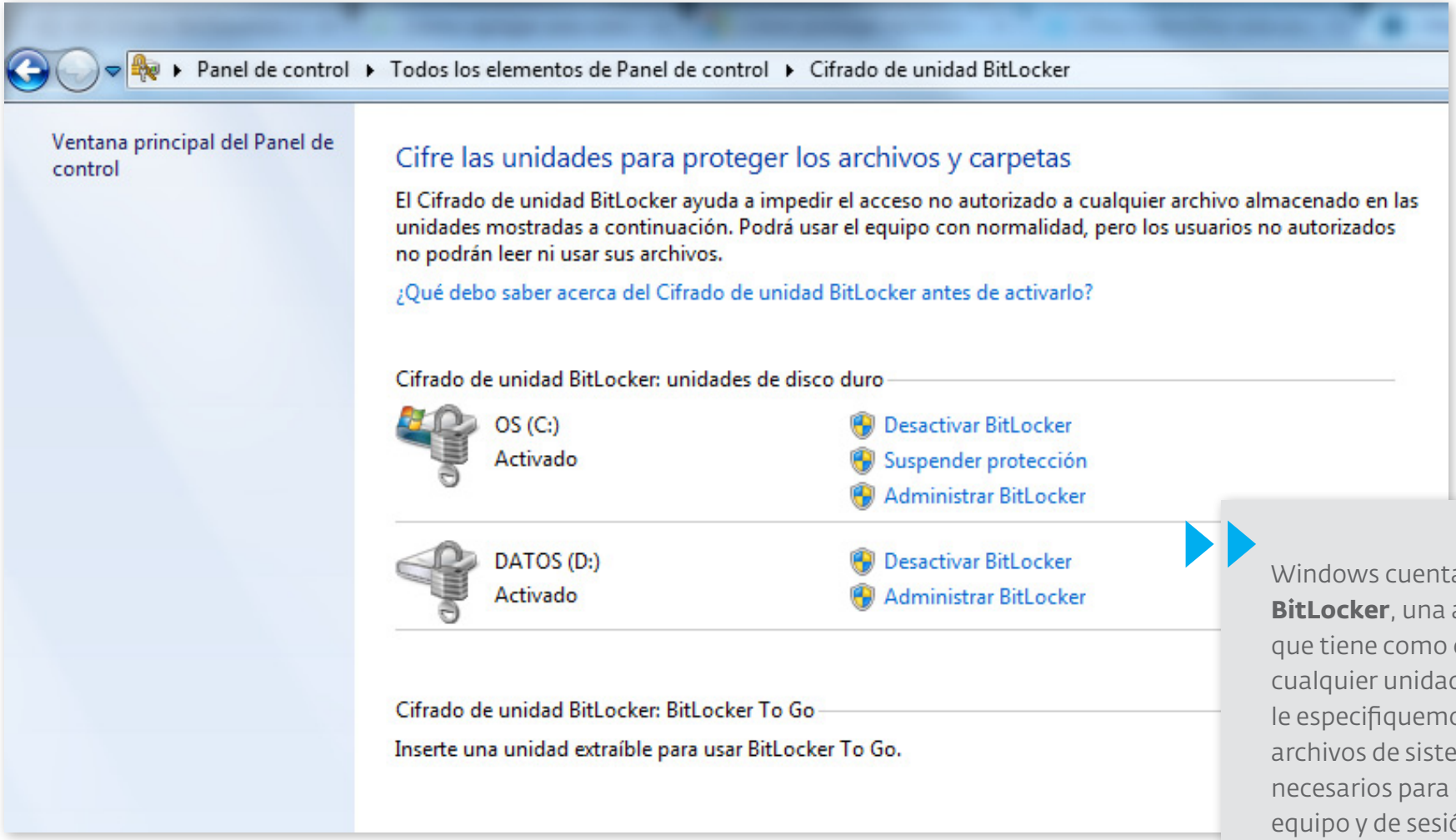
Cifrando la información en computadoras

Los principales espacios de almacenamiento se encuentran en computadoras o en dispositivos accedidos por estas. Por lo tanto, es muy importante tener especial **cuidado al momento de cifrar** estos grandes repositorios de información.

En caso de que la computadora se pierda, o incluso para evitar un acceso indebido a la información, muchas veces **no basta tener una contraseña de acceso como la única medida de protección**. Una buena alternativa es utilizar las **opciones de cifrado de datos que ofrece el sistema operativo** que tenga el equipo.

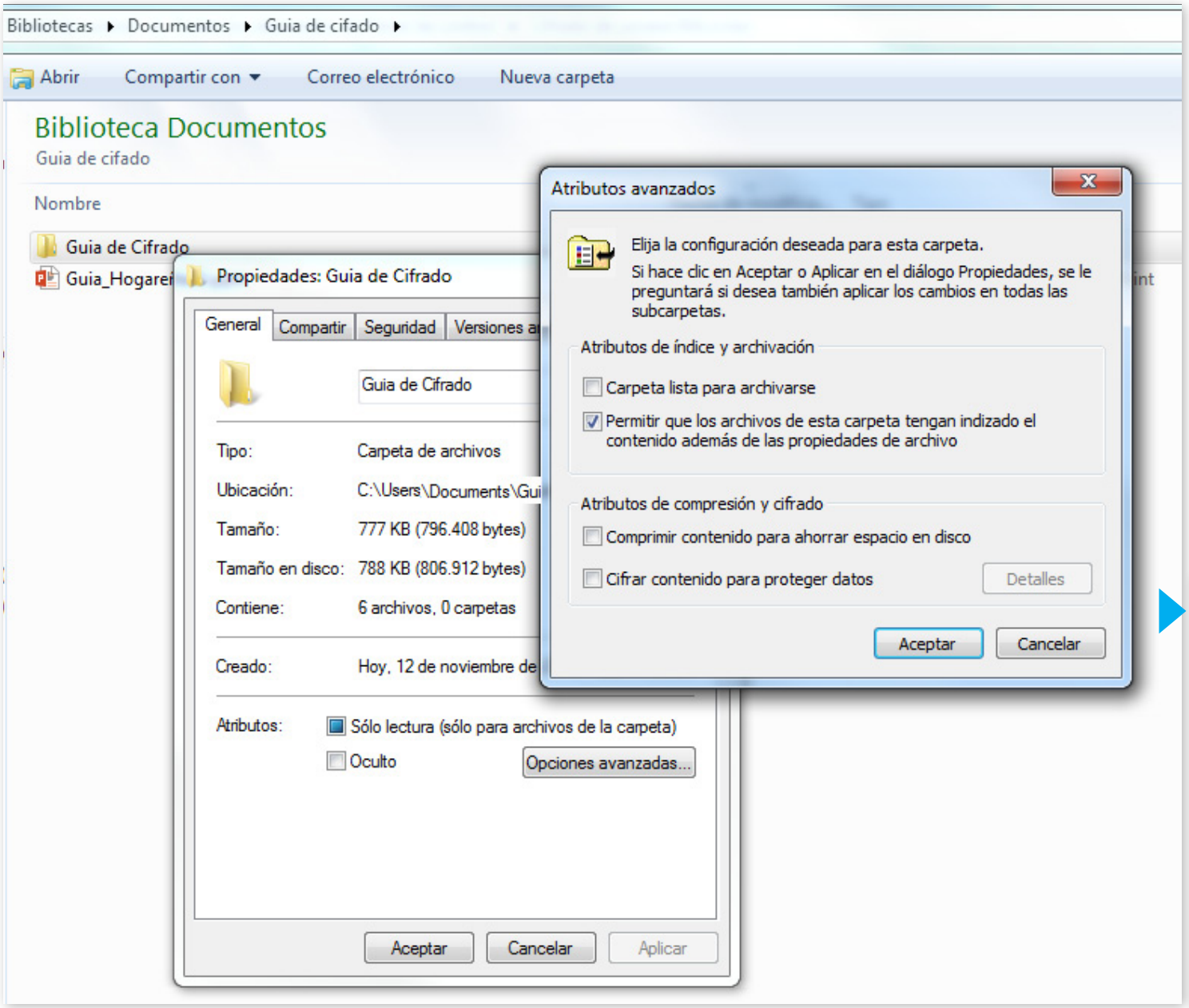
El uso de **archivos comprimidos con clave** es una alternativa práctica para intercambiar información. Cabe destacar que la contraseña utilizada para proteger la información debe ser lo **suficientemente robusta** y que el algoritmo utilizado por el software sea lo suficientemente seguro.

Cifrado en Windows



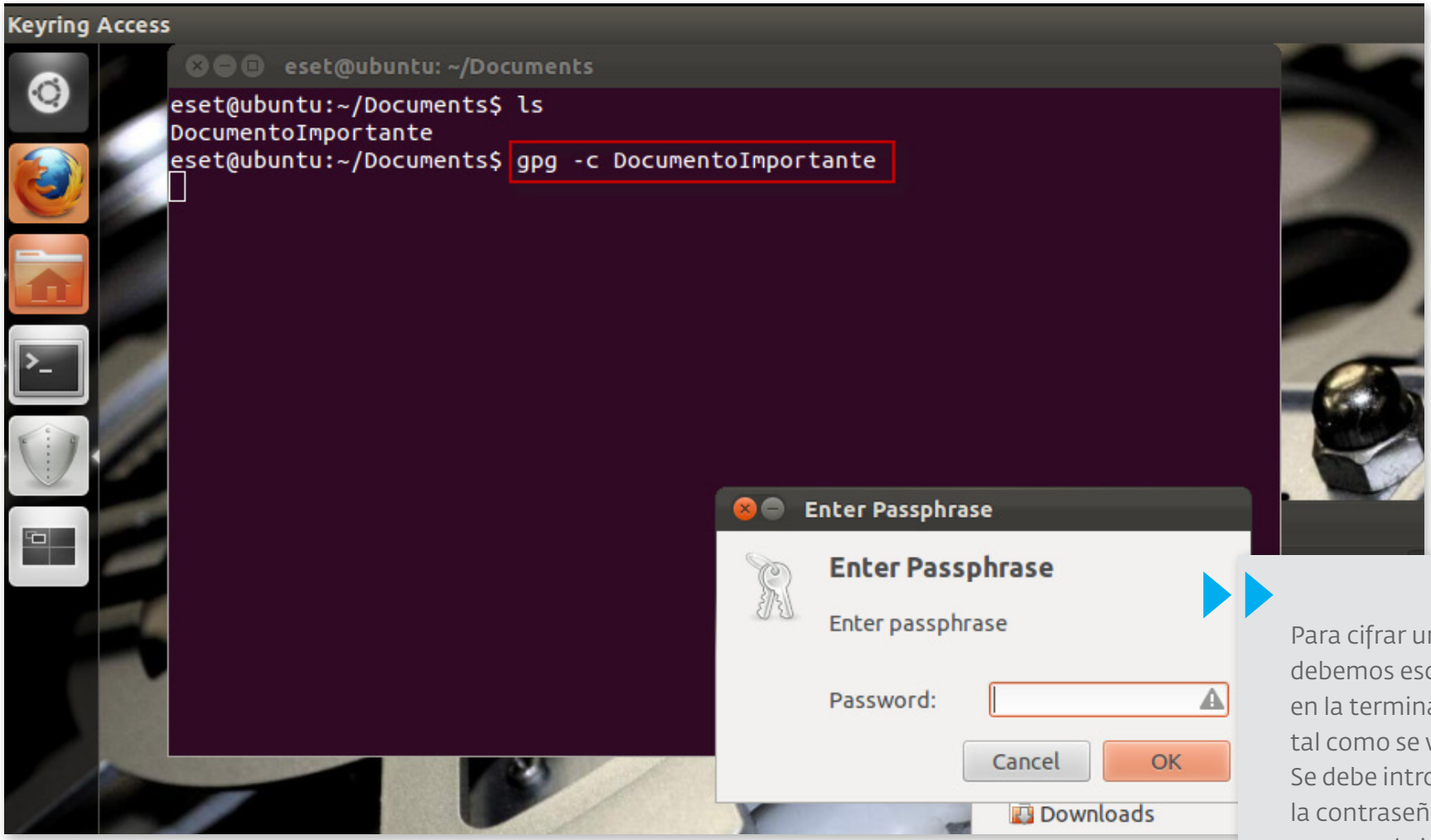
Windows cuenta con **BitLocker**, una aplicación que tiene como objetivo cifrar cualquier unidad de disco que le especifiquemos, incluidos los archivos de sistema de Windows necesarios para el inicio del equipo y de sesión contenidos en el disco de arranque del sistema.

Cifrado en Windows



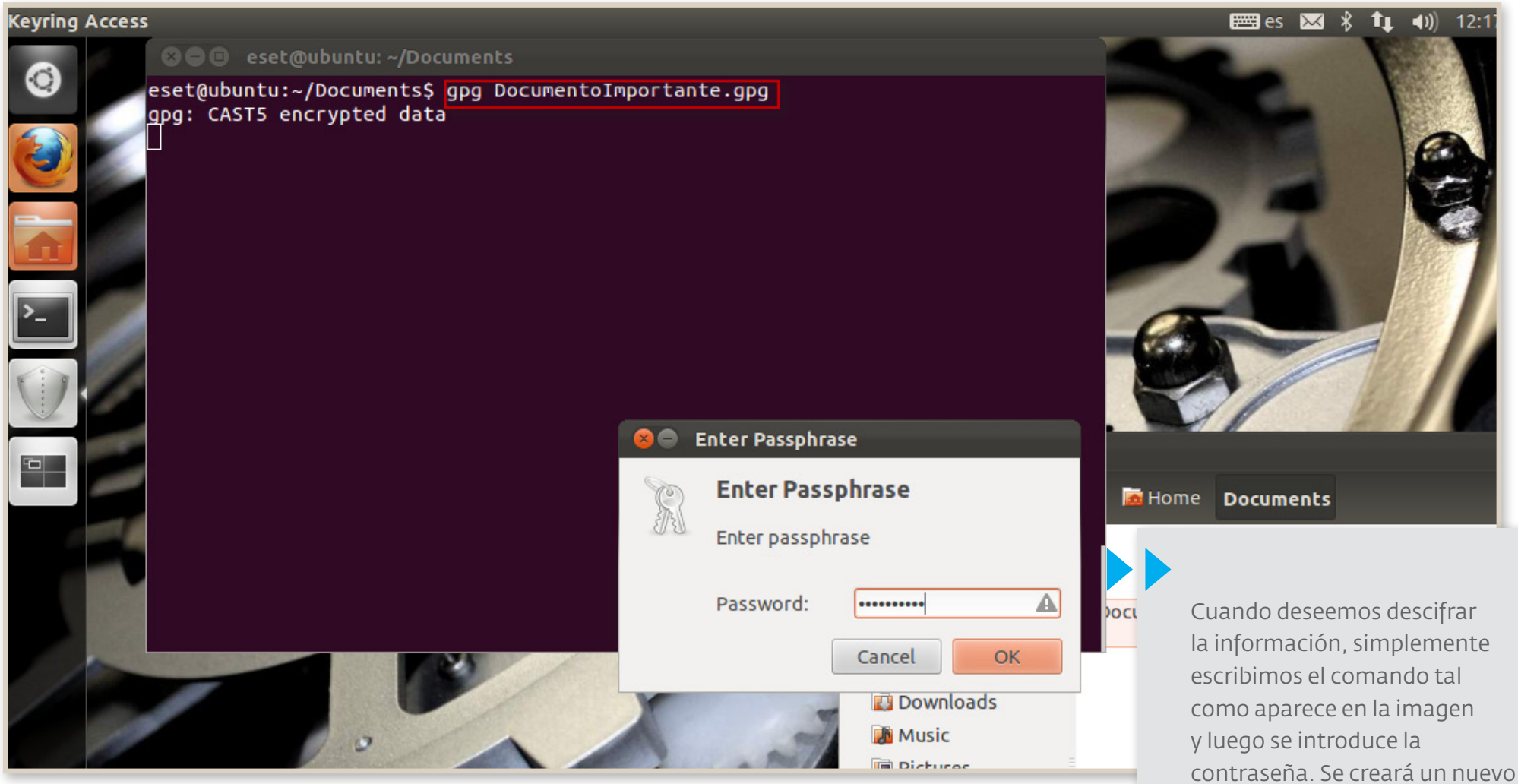
Windows también cuenta con una característica que nos permite cifrar archivos alojados en nuestra computadora individualmente. Basta con activar una casilla en las propiedades del archivo o de la carpeta específica que deseemos cifrar.

Cifrado en Linux



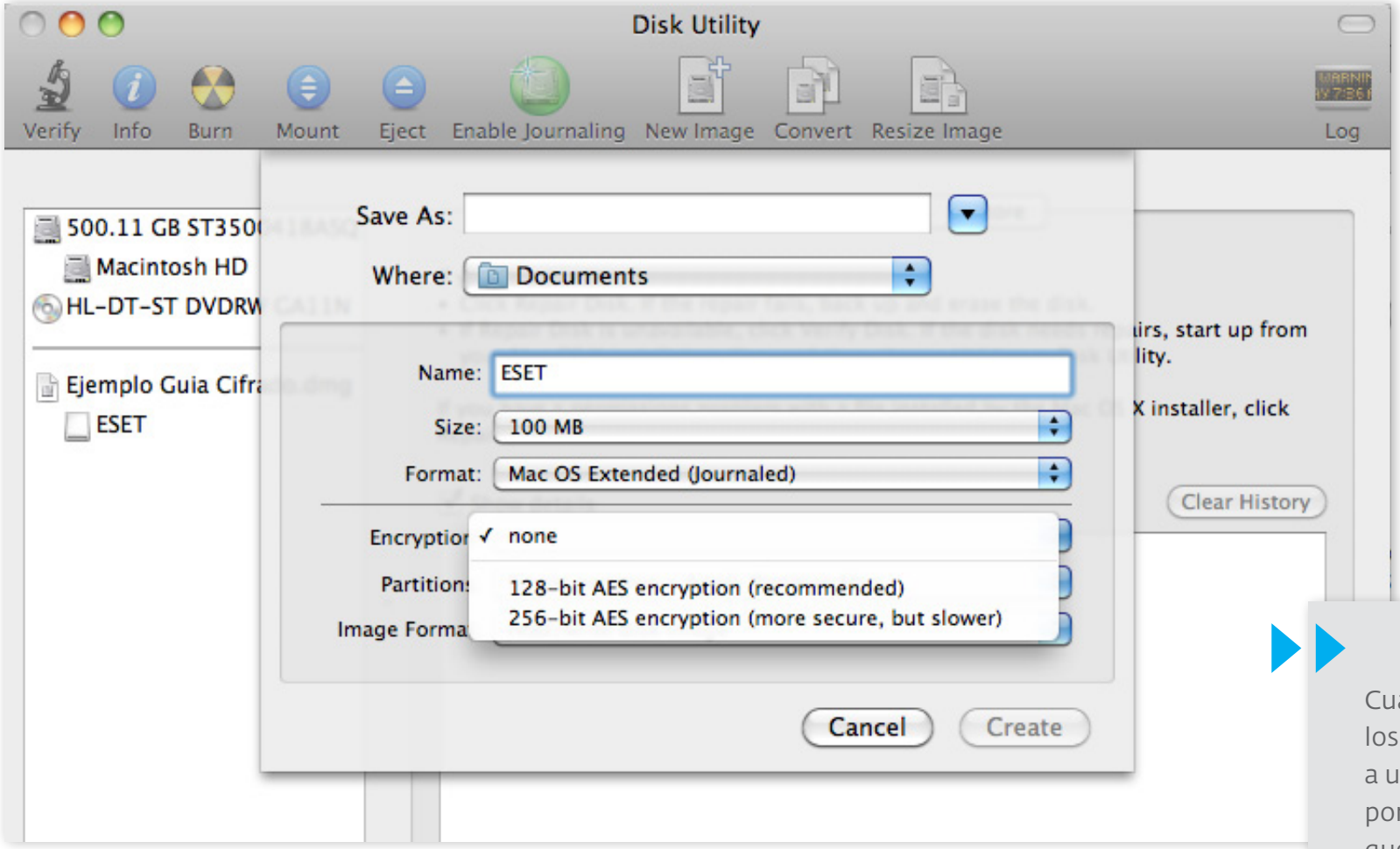
Para cifrar un archivo en Linux, debemos escribir el comando en la terminal de Ubuntu, tal como se ve en la imagen. Se debe introducir dos veces la contraseña que sirve para proteger la información, luego de lo cual se crea un nuevo archivo con extensión *.gpg*.

Cifrado en Linux



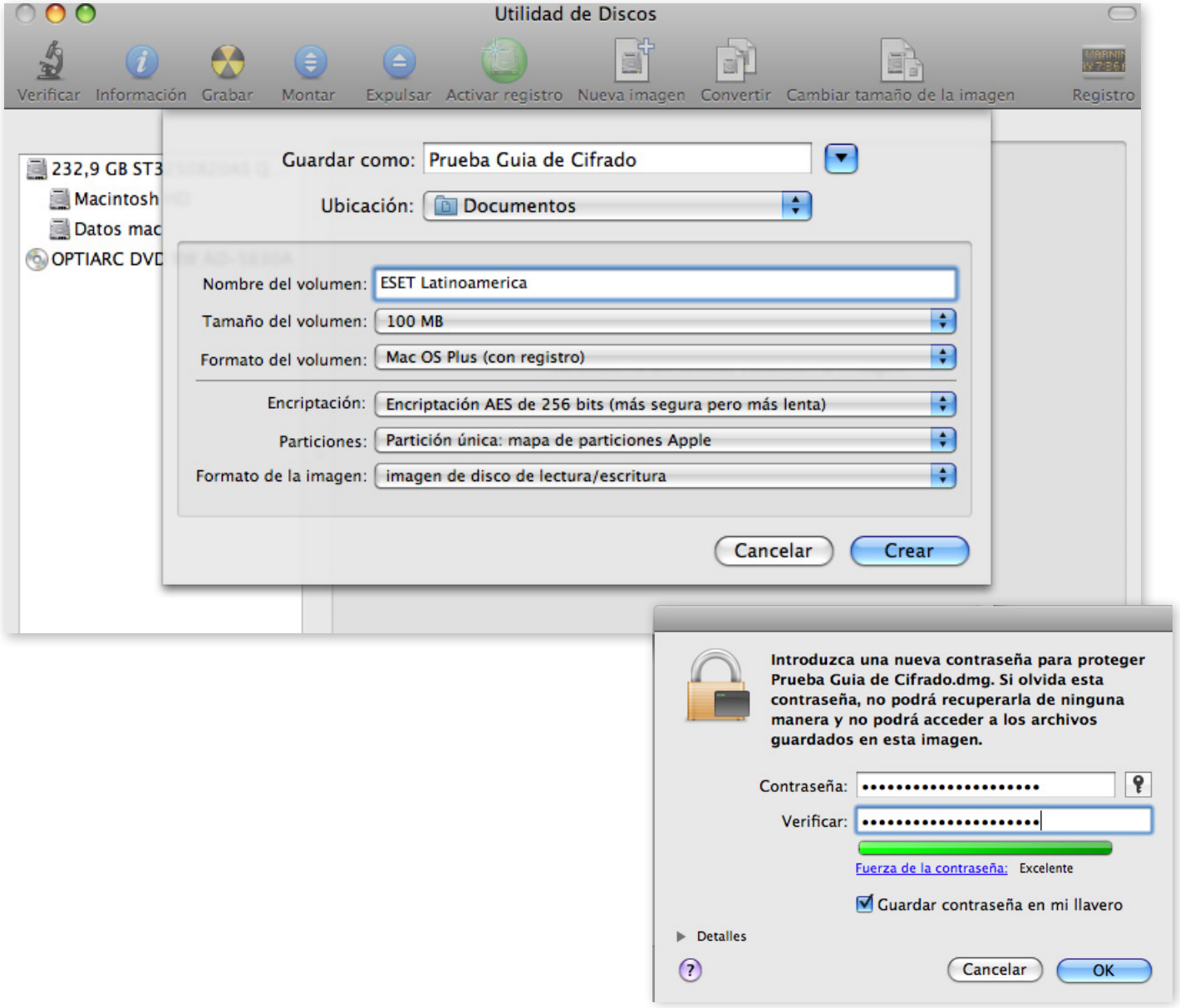
Cuando deseemos descifrar la información, simplemente escribimos el comando tal como aparece en la imagen y luego se introduce la contraseña. Se creará un nuevo archivo con la información lista para ser leída.

Cifrado en Mac OS X



Cuando se cifra la información, los datos se alteran de acuerdo a un patrón establecido por una clave, de tal forma que solamente puedan ser entendidos por quienes conocen esa clave.

Cifrado en Mac OS X



Así, un mensaje cifrado puede ser enviado de un lugar a otro o almacenado en algún dispositivo. Si alguien accede a ese archivo sin poseer la clave, no podrá ver la información.

No obstante, existen ataques para intentar acceder a esos archivos sin la clave. La dificultad para descifrar la información a partir de un ataque dependerá de la forma de cifrado, la información y la clave utilizada.

Y en dispositivos móviles, ¿hay información para cifrar?

¿Qué tipo de actividades realizas con tu dispositivo móvil, sea Smartphone o Tablet? Si comparamos la respuesta con los usos que hacemos de nuestras computadoras, seguramente **no encontraremos mayores diferencias**. Esto indica que también almacenamos y manejamos información importante en los dispositivos móviles.

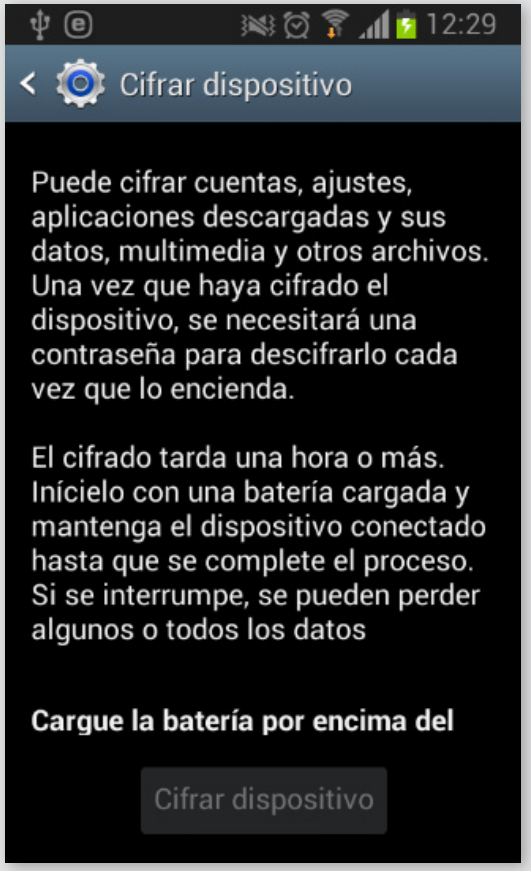
Sin embargo, estos dispositivos están **más expuestos al robo o extravío**, pues los tenemos todo el tiempo con nosotros. Por esta razón, es fundamental que el dispositivo cuente con, al menos, una **clave de acceso**. De esta forma, impedimos que un tercero pueda acceder a nuestras fotos, videos, contactos y cualquier otra información alojada allí.

Existe otra variable que considerar: el **medio de intercambio de información** más utilizado por estos dispositivos es el aire, por lo que cualquiera podría estar monitoreando las señales de las diferentes redes. A raíz de esto, es necesario tener mucho cuidado en las redes utilizadas para intercambiar información, y es recomendable utilizar **canales cifrados** cuando se trata de información confidencial.

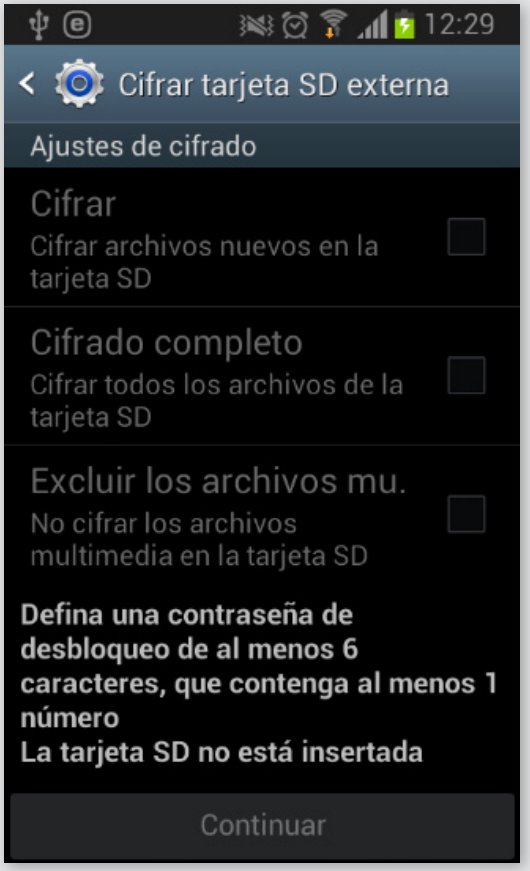
Al igual que para las computadoras, los principales fabricantes de dispositivos móviles cuentan con **herramientas de cifrado nativas** de cada sistema operativo.

Cifrado en Android

Android ofrece una herramienta de Cifrado en el menú Ajustes/Seguridad, para cifrar la información del dispositivo y de la tarjeta SD. Ambos casos requieren contraseña, por lo que es aconsejable que sea fuerte para mayor seguridad.



Cuando se selecciona la opción de *Cifrar dispositivo* las cuentas, los ajustes, las aplicaciones descargadas, las fotos, videos y otros archivos multimedia quedarán cifrados.



En la opción *Cifrar tarjeta SD externa* se pueden seleccionar los archivos a cifrar: los nuevos, todos los archivos o excluir los archivos multimedia.

Cifrado en iOS

Los dispositivos móviles que utilizan como sistema operativo iOS, **traen encriptada la información** con AES 256 y además usan Data Protection para **cifrar todas las comunicaciones** entrantes y salientes.

Esta característica implementada por Apple, tiene además un sistema de Número Personal de Identificación que automáticamente **borra todo el contenido** del dispositivo después de **diez intentos fallidos** por adivinarlo.

La clave del algoritmo es diferente para cada dispositivo y está insertada directamente en el hardware.

El cifrado como una medida más de protección

El cifrado de la información es una práctica que se ha **popularizado** cada vez más, tanto en ambientes corporativos como hogareños, debido al **uso intensivo de la tecnología** por parte de los usuarios y a la **confluencia del ámbito personal y laboral en un mismo dispositivo**.

Sin embargo, esta evolución conlleva un **crecimiento de las amenazas informáticas**. No es solamente el robo o extravío del dispositivo lo que puede generar que perdamos nuestra información, sino también códigos maliciosos, vulnerabilidades, ataques dirigidos, ingeniería social, etc.

Por esta razón, la protección **debe ser integral**; y para lograrla, es aconsejable utilizar una **solución de seguridad** y verificar que las aplicaciones siempre provengan de las **fuentes oficiales**.

De este modo, se puede aplicar el **cifrado** de la información sensible del dispositivo como una **capa adicional de protección** para disfrutar de las tecnologías de una forma más segura.

ENJOY SAFER TECHNOLOGY™

www.eset-la.com

/esetla

@esetla

/company/eset-latinoamerica