Guía para el cifrado de la información

Todos estamos expuestos a la pérdida o robo de información de carácter privado o confidencial al hacer uso de las redes de datos y de dispositivos o soportes externos. Esta guía está pensada para mantener a salvo la privacidad y la seguridad de la información.

Cuándo cifrar

Las técnicas de cifrado permiten transformar el contenido de archivos o documentos de manera que sean incomprensibles para cualquier persona que no disponga de la contraseña o certificado empleado para el cifrado.

La información se protegerá mediante la utilización de técnicas de cifrado cuando se almacenen o trasladen ficheros sujetos a condiciones de **nivel alto de seguridad**, contengan o no datos personales.

El cifrado de información es un proceso muy sensible y de alto riesgo, ya que, si se perdiese la contraseña de generación del cifrado o el certificado fuese revocado, no se podría recuperar la información cifrada. Por ello, se recomienda utilizar cifrado sólo en aquellos casos en que está previsto por las distintas normativas y leyes que lo requieran. A este respecto, y teniendo en cuenta el Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD), los casos en que se debe cifrar la información son los siguientes:

1) Referencias en el **ENS**:
    a. Sobre el cifrado de la información (mp.info.3), “la información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella”.
    b. Sobre la protección de la confidencialidad e integridad (mp.si.2) en dispositivos removibles (CDs, DVDs, discos USB u otros de naturaleza análoga) que contengan información de nivel medio o alto, se aplicarán mecanismos criptográficos.
    c. Sobre la protección de portátiles (mp.eq.3), “la información de nivel alto almacenada en el disco se protegerá mediante cifrado”.
2) Referencia en la nueva **LOPD**:

a. Sobre medidas de seguridad en el ámbito del sector público (Disposición adicional primera): se deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

En consecuencia, toda información clasificada como confidencial, reservada o de nivel alto con respecto a Protección de Datos o ENS, deberá encontrarse cifrada, tanto en su almacenamiento (PC sobremesa, portátil, USB, DVD, etc.), como en su envío a través de medios electrónicos (servicios de correo electrónico, consigna, espacios colaborativos, etc).

En cualquier caso, el propio usuario puede decidir la aplicación del cifrado de su información aún cuando no sea estrictamente necesario según las normativas y leyes a las que queda obligado.

Qué cifrar

A la hora de cifrar la información se tendrán en cuenta las siguientes opciones:

1) Se puede cifrar todo el disco (sistema operativo, aplicaciones y datos), en el caso de portátiles/PCs y USBs
2) Se puede cifrar únicamente una partición/carpeta/ficheros en cualquier equipo, pero habrá que tener en cuenta que, en caso de robo del mismo, si no se cifra la parte del sistema operativo, sería posible acceder a información de carácter personal
3) Se pueden cifrar documentos de forma individual utilizando aplicaciones como Office, Adobe PDF, ZIP, etc.
4) Se pueden cifrar las comunicaciones utilizando aplicaciones y protocolos seguros (por ejemplo, https en vez de http para web).

Para cifrar información se pueden utilizar tanto contraseñas como certificados digitales para asegurar la identidad de la persona que nos envía información cifrada.

Cómo cifrar

Existen numerosas herramientas para el cifrado de la información, tanto almacenada como en tránsito. Debido a la continua evolución de los programas y herramientas de cifrado, es difícil mantener una lista actualizada. En el Anexo I se incluyen algunas herramientas de software libre, tanto para cifrar archivos en distintos sistemas operativos, como para cifrar las comunicaciones.

Riesgos de cifrar

Una vez analizadas las ventajas de utilizar un sistema de cifrado para preservar la confidencialidad de la información se deben analizar los riesgos que esta técnica conlleva:

- Pérdida u olvido de la contraseña de cifrado: el riesgo se evita cifrando sólo la información que lo requiera y estableciendo, antes de cifrar, una vía de recuperación alternativa que permita acceder a la información en caso de pérdida de la contraseña.
- Baja calidad de la contraseña: se evita usando una contraseña robusta.
- Gestión indebida de contraseñas: si no se administran las contraseñas de cifrado adecuadamente puede ponerse en peligro la integridad, confidencialidad y disponibilidad de la información. Las claves que existen en sistemas basados exclusivamente en software son vulnerables a ataques.
- Decisión de cifrado por parte del usuario final: si no existe una directiva clara acerca de la información que hay que cifrar, se puede incurrir en faltas legales con el consecuente riesgo de multas y daños en los Servicios.
- Revocación o caducidad de certificados de servidor utilizados en el cifrado de las comunicaciones: la seguridad no está garantizada si no se verifica la integridad y validez del certificado y si el emisor del mismo no es una autoridad de certificación (CA) de confianza.

Anexo I: Algunas herramientas de cifrado

DiskCryptor es una solución Open Source para el cifrado de particiones y discos duros completos para Windows, permitiendo también el cifrado de particiones individuales incluyendo la partición donde está instalado el sistema operativo. Permite cifrar archivos, particiones o dispositivos de almacenamiento externo USB. También incluye algoritmos de cifrado tales como AES, Twofish, Serpen o una combinación de algoritmos en cascada en el modo XTS para llevar a cabo el cifrado y está publicado bajo una licencia GPLv3.

AES Crypt es un software de cifrado de archivos que utiliza el estándar *Advanced Encryption Standard* también conocido como *Rijndael*, para cifrar archivos de forma fácil y segura. Esta herramienta se ejecuta desde la línea de comandos en Linux y se integra con la *shell* Windows. Todos los archivos y directorios cifrados con *AES Crypt* son accesibles mediante una contraseña, eliminando así los accesos no autorizados. También dispone de una biblioteca para los desarrolladores que utilizan *Java* para leer y escribir archivos con formato AES.

EncFS proporciona un sistema de archivos cifrado en el espacio del usuario. No requiere permisos especiales y está basado en el módulo *FUSE* para proporcionar la interface del sistema de ficheros. Son dos los directorios involucrados en el montaje de un sistema de archivos EncFS: el directorio de origen y el punto de montaje. Los archivos son cifrados mediante una clave del volumen que se almacena cifrada en el directorio de origen y es necesaria una contraseña para

descifrarla. EncFS es un software gratuito bajo licencia GPL disponible en sistemas Linux, BSD y Windows.

VeraCrypt es una solución de cifrado Open Source basada en TrueCrypt. Utiliza la misma interfaz y características con la diferencia que incluye un número mayor de iteraciones para el cifrado de la información. La desventaja del aumento significativo de iteraciones es que VeraCrypt es más lento al momento de implementar lectura y escritura de información en el disco. Al igual que TrueCrypt, VeraCrypt incluye algoritmos de cifrado tales como AES, Twofish y Serpent.

OpenStego es una herramienta Open Source para Windows y Linux que permite utilizar la técnica de estenografía (rama de la criptografía) para guardar información de manera segura a través de imágenes, música y/o videos. En términos simples, con OpenStego podemos enviar mensajes ocultos dentro de una imagen o cualquier archivo multimedia.

OpenPuff es una herramienta Open Source para Windows de Estenografía. Fue una de las primeras herramientas de estenografía. Soporta imágenes en formato BMP y JPG, archivos de audio MP3 y WAV, archivos de video MPG4, entre otros.

GNUGPG es una implementación libre de PGP (Pretty Good Privacy). GNUGPG permite el cifrado y firma de datos y de las comunicaciones. Utiliza el estándar del IETF denominado OpenPGP y es software libre bajo la licencia GPL. GPG, como también se le conoce, es una herramienta basada en la línea de comandos que te permite cifrar y firmar tus datos y comunicaciones. Cuenta con un sistema de llave versátil de gestión, así como módulos de acceso para todo tipo de directorios de claves públicas. También dispone de varias funciones que facilitan su integración con otras aplicaciones y su versión 2 presta soporte a S/MIME, un estándar de criptografía para correo electrónico.

OpenSSH es una herramienta Open Source de acceso remoto a través del protocolo IP. OpenSSH es la alternativa perfecta al protocolo Telnet. Con OpenSSH podemos conectarnos de manera segura a un dispositivo en la red, ya que la información que viaja entre ambos nodos va cifrada utilizando algoritmos de cifrado simétricos. OpenSSH también incluye capacidad de Tunneling y autenticación.

OpenSSL es un la implementación Open Source del protocolo SSL (Secure Socket Layer). Este protocolo permite el cifrado de información a través de la red. Viene instalado en prácticamente el 99% de todos los navegadores web. Este SSL protocolo es utilizado para realizar de manera segura la mayoría de transacciones en línea. OpenSSL es también utilizado como solución de

VPN (Virtual Private Network) como alternativa al protocolo IPSEC, principalmente en la conectividad de usuarios remotos.

Además de estas y otras muchas herramientas de cifrado disponibles en Internet, existen aplicaciones como MS Office, OpenOffice, Adobe PDF, ZIP, etc. o funciones de los distintos sistemas operativos, que permiten encriptar documentos de forma individual.