# Cifrado de la información

## Guía corporativa

ENJOY SAFER TECHNOLOGY™

# La encriptación de datos en las empresas

# 1. Introducción

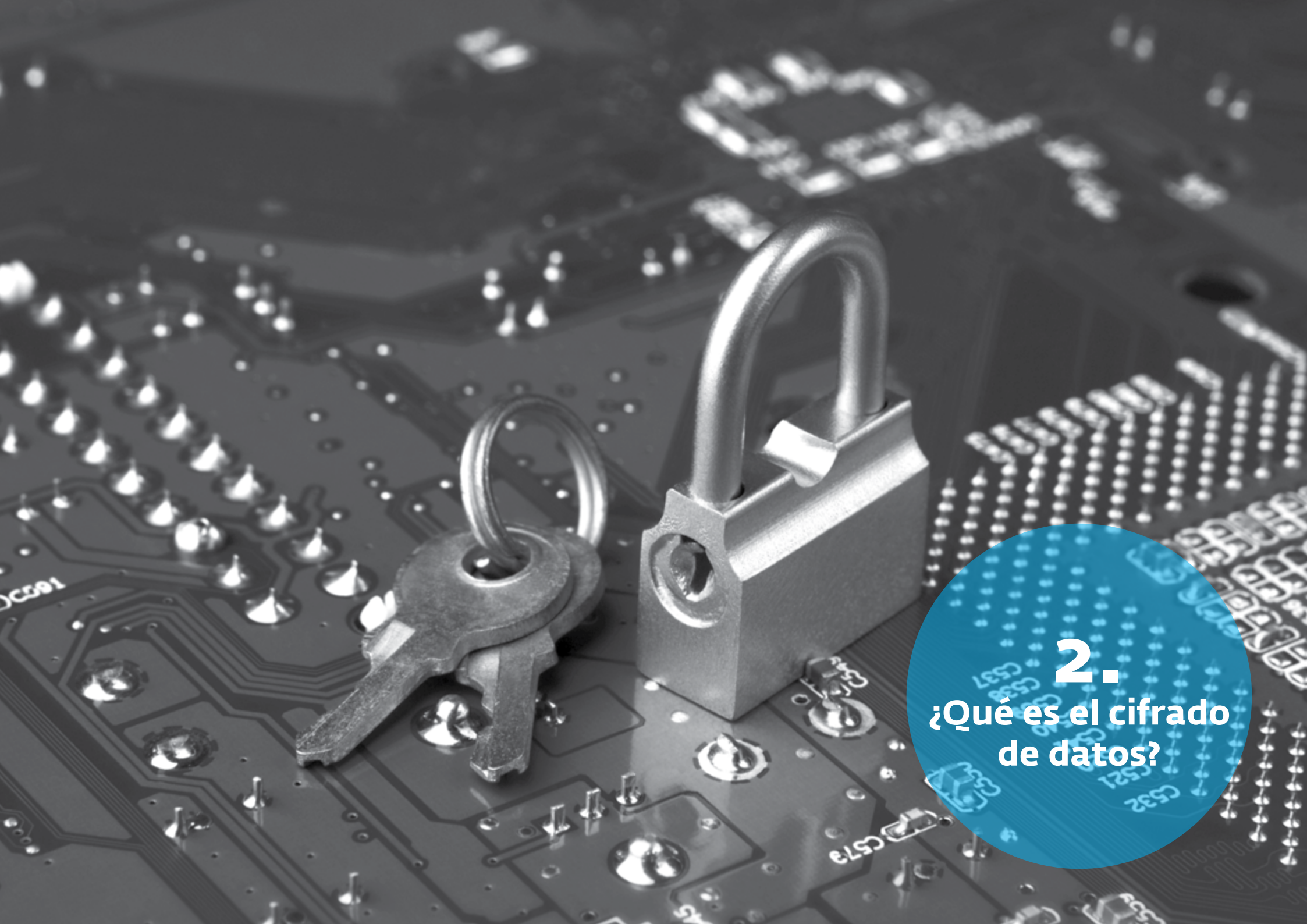
# 1. Introducción

La información es uno de los recursos más importantes en una empresa, desde la más pequeña hasta la más grande. Por ello, es indispensable protegerla ante todos los riesgos que existen.

De esta manera, manejar adecuadamente la información puede hacer que la compañía no sufra de las consecuencias de un ataque, principalmente en términos de prestigio y confianza de sus clientes.

Actualmente, las amenazas a la información corporativa incluyen desde el malware y la explotación de vulnerabilidades, hasta el robo de dispositivos móviles. Además, teniendo en cuenta que el tema de la privacidad de las comunicaciones está en pleno debate internacional, el concepto de cifrado de datos se popularizó como una forma de mantener la información segura, tanto el ámbito hogareño como en el corporativo.

El objetivo de esta guía es profundizar en el tema de la encriptación de la información y, de ese modo, poder exponer y explicar los beneficios que ofrece a las empresas.



# 2.
## ¿Qué es el cifrado de datos?

# 2. ¿Qué es el cifrado de datos?

Cifrar o encriptar datos significa alterarlos, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original.

Esta técnica protege la información sensible de una organización, ya que si los datos cifrados son interceptados, no podrán ser leídos.

**Una de las primeras técnicas de cifrado que se usó en la historia fue el "código del César", que consistía en reemplazar cada letra de un mensaje por otra que se encontrara más adelante en el alfabeto. Debido a su baja complejidad, se idearon otros métodos, por ejemplo, tatuar las claves de descifrado en los esclavos.**

# 3.
# ¿Por qué es necesario cifrar los datos?

# 3. ¿Por qué es necesario cifrar los datos?

Cifrar los datos implica que cada vez que se quiera acceder a los mismos, se deban descifrar, lo que agrega un nivel de complejidad al acceso simple, pero reduce la velocidad del proceso. A raíz de esto, surgen ciertas preguntas: ¿por qué hay que cifrar la información importante en una empresa? ¿Cuáles son los beneficios de hacerlo?

**En septiembre de 2011, la empresa holandesa DigiNotar tuvo que declararse en bancarrota, tras haber sufrido un ataque de fuga de información.***

Es muy difícil para una compañía poder revertir el daño generado luego de una intrusión significativa, por lo que es fundamental tomar las medidas necesarias para evitarlas y, si ocurren, contar con la preparación adecuada para minimizar el riesgo, por ejemplo, utilizando datos cifrados.

*Fuente: http://blogs.eset-la.com/laboratorio/2011/10/07/ataque-informatico-lleva-diginotar-quiebra/


# 4.
# Beneficios del cifrado

# 4. Beneficios del cifrado

A. **Proteger la información confidencial de una organización:** si la información sensible de una compañía llegara a caer en las manos equivocadas, pueden producirse perjuicios económicos, pérdidas de ventaja competitiva, o incluso significar el cierre de la empresa. En este sentido, la encriptación ayuda a proteger Información delicada, como los datos financieros, de los colaboradores, procedimientos o políticas internas, entre otros.

B. **Proteger la imagen y el prestigio de una organización:** existe cierta información que si es robada, puede dañar la imagen corporativa. Un ejemplo notable, son los datos que se almacenan de los clientes; el robo de los mismos puede afectar considerablemente a la empresa, llevándola a pérdidas irrecuperables.

C. **Proteger las comunicaciones de una organización:** el cifrado es comúnmente asociado con las transmisiones de datos, dado que los mensajes enviados por una empresa suelen viajar por canales o infraestructura externa, como Internet, y son susceptibles a ser interceptados. El ejemplo más significativo, es el cifrado de los mensajes enviados por correo electrónico.

D. **Proteger dispositivos móviles e inalámbricos:** todos aquellos dispositivos que salen de la empresa, como teléfonos celulares, tablets o computadoras portátiles, pueden ser extraviados y/o robados. Ante estas situaciones, es importante asegurarse de que ningún tercero esté autorizado pueda acceder a la información.


## 5.
## ¿Qué rol juega la clave en el cifrado?

# 5. ¿Qué rol juega la clave en el cifrado?

La clave es una parte esencial del mecanismo de cifrado de datos, ya que representa la única posibilidad de descifrar la información y, por tanto, leerla. Por ello, resulta fundamental escoger una clave robusta, ya que significará que la barrera entre los datos y los intrusos será más difícil de cruzar.

Elegir una clave como "1234" o "secreta" es sumamente inseguro, ya que si bien son fáciles de recordar, son igualmente fáciles de adivinar, motivo por el cual no representan ninguna garantía de protección de los datos. Ahora bien, una clave ideal sería aquella cuya longitud fuese lo más larga posible, y su contenido lo más aleatorio posible; sin embargo, este tipo de claves son difíciles de recordar.

**En febrero de 2013, Burger King sufrió un ataque en el que lograron acceder y tomar control de su cuenta oficial de Twitter. Los atacantes cambiaron el aspecto de la cuenta y mostraron imágenes de su principal competidor. Aparentemente, el ataque se perpetró por una contraseña débil; una alternativa para evitar esto es el uso de una contraseña fuerte y contenida en un almacén de claves que también debe estar cifrado.***

**Fuente: http://blogs.eset-la.com/laboratorio/2013/02/18/burger-king-o-mcdonalds-o-como-una-contrasena- debil-en-twitter-puede-danar-tu-imagen/*

# 6.
# Consideraciones para definir una clave de cifrado

# 6. Consideraciones para definir una clave de cifrado

A. **No utilizar palabras reconocibles:** existe un tipo de ataque utilizado para adivinar una clave que consiste en probar una por una las palabras de un diccionario (y combinaciones de ellas) hasta encontrar una que coincida con la clave.

B. **No utilizar claves demasiado cortas:** el ataque por fuerza bruta prueba todas las combinaciones de caracteres posibles hasta encontrar la clave. Así, a medida que se incrementa la cantidad de caracteres en la clave, el tiempo necesario para probar todas las combinaciones crece de manera exponencial. Mientras más larga sea la clave, será más difícil que sea descubierta por un ataque de fuerza bruta, con la tecnología actual.

C. **Utilizar minúsculas, mayúsculas, números y caracteres especiales:** al igual que en el punto anterior, el ataque de fuerza bruta puede reducirse a través de la variedad de caracteres, ya que implica más pruebas de combinaciones.


D. **No utilizar datos públicos:** si bien esto es muy común, debe ser evitado. La dirección de la empresa, la fecha de aniversario, el nombre, entre otros, son ejemplos típicos.

E. **Utilizar una solución para el manejo seguro de las claves:** una buena idea es apoyarse en el uso de una herramienta de gestión de claves. Este tipo de aplicaciones proveen mecanismos para generar claves seguras y almacenarlas en un depósito centralizado. En este caso sólo es necesario recordar una clave, la del acceso al depósito, la cual debería seguir los lineamientos mencionados previamente.

# 7.-

## ¿Qué tipo de información debe ser cifrada?

# 7. ¿Qué tipo de información debe ser cifrada?

La información sensible de una empresa está presente en una gran variedad de formas y se transmite o almacena en diversos dispositivos. A su vez, es necesario tener en cuenta el criterio para cifrar los datos responde al valor que tienen para el negocio.

En primera instancia, la información que se envía en una transmisión de datos puede ser cifrada, ya que los canales a través de los que viaja un mensaje no pertenecen a la empresa, y es posible que alguien no deseado intercepte el mensaje. Por ello, la implementación del cifrado de los mensajes garantiza que solo aquellos que posean la clave puedan descifrar el mensaje y acceder a su contenido.

Luego, existe información sumamente importante que, si bien es almacenada en dispositivos de la empresa y no es transmitida, también corre riesgo de ser accedida por terceros. Un ejemplo típico es el de las computadoras portátiles, que solo son accedidas por sus dueños, pero existe el riesgo de sean robadas o extraviadas, motivo por el cual la información debe estar debidamente protegida. De igual forma, la información que se encuentra almacenada en servidores de la empresa podría ser accedida si no se toman los recaudos necesarios.

Por último, vale la pena mencionar el caso de los smartphones y tablets. Este tipo de dispositivos son cada vez más comunes en el ámbito corporativo, tanto para la transmisión de datos como para el almacenamiento de documentos de trabajo. Por lo tanto, deben ser tenidos en cuenta al momento de definir qué información se va a cifrar.

Solo el 20% de las empresas de Latinoamérica utilizan cifrado para proteger su información, de acuerdo con el ESET Security Report 2013.*

*Fuente: http://www.eset-la.com/centro-amenazas/descarga/Latinoamerica-2013/3107

# 8.
# Cifrado de las comunicaciones

# 8. Cifrado de las comunicaciones

## • A. Correo electrónico •

Una forma de cifrar los mensajes de correo electrónico es utilizando una clave privada. Este método es el más fácil de implementar y consiste en cifrar el texto en cuestión para luego enviarlo dentro del correo; así, el destinatario debe conocer la clave para poder obtener el mensaje original. Sin embargo, cada vez que se quiera enviar un mensaje cifrado a alguien que no conozca la clave, se deberá comunicar la misma por algún medio seguro.

Ante la incertidumbre acerca de cómo transmitir la clave de forma segura, surge la alternativa del cifrado con clave pública. Este sistema es más robusto y se basa en la utilización de certificados: tanto el emisor como el receptor tienen su propio certificado que pueden publicar sin comprometer su seguridad. Así, cada vez que se quiera enviar un mensaje a alguien, se cifrará el mismo con la clave pública establecida en el certificado del destinatario. En el otro extremo, al recibir un mensaje cifrado se le aplicará una clave secreta que no conoce nadie, para obtener el mensaje original. En resumen, la clave con la que se cifra es distinta a aquella con la que se descifra y, si bien están relacionadas, no se puede obtener una conociendo la otra.

Una vez que un usuario tiene su propio certificado válido, deberá intercambiar mensajes digitalmente firmados con sus contactos, para obtener y almacenar los certificados de ellos. A partir de allí, el proceso de cifrado será prácticamente transparente para el usuario. En el caso en que se quiera enviar un mensaje cifrado y el destinatario no cuente con la posibilidad de leerlo, se le dará la opción al emisor de enviar el mensaje sin cifrar.

**El caso PRISM y los programas de espionaje de agencias gubernamentales han puesto el tema de la privacidad en Internet en el centro del debate, popularizando el cifrado de datos como una alternativa para la protección de los correos electrónicos y demás comunicaciones.**

La forma más conveniente de implementar el cifrado de correos electrónicos es a través de componentes o plugins que se integren a los servicios de correo electrónico como Outlook.

Así, el manejo de claves compartidas y el proceso de cifrado serán transparentes al usuario.

# 8. Cifrado de las comunicaciones

## • *B. Navegación cifrada para los clientes* •

Cuando los clientes navegan por el sitio web de una empresa, realizan envíos y solicitudes constantes de información, que en muchos casos puede ser confidencial o de alto valor para el cliente, por lo que se hace necesario brindarle un mecanismo de seguridad para protegerlas. Una forma muy utilizada es a través del cifrado de los datos que se envían.

En este caso, el proceso de cifrado es similar al que se describió para el envío de correos electrónicos, mediante la utilización de certificados. Por ello, para poder brindar este mecanismo de seguridad a los usuarios, se hace necesario contar con un certificado que identifique a la empresa y su sitio web, el cual será obtenido de una Autoridad de Certificados.

La aplicación más común de la navegación cifrada se da a la hora de realizar el ingreso de datos bancarios o tarjetas de crédito, pero también puede aplicarse a toda una sesión de navegación: cuando un usuario registrado quiere autenticarse se realiza el intercambio de certificados y el establecimiento de la conexión segura; la comunicación cifrada, entonces, se mantendrá hasta el cierre de sesión.

**Hasta hace algunos años, la navegación segura se veía en pocos sitios. Por ejemplo, Facebook la implementó en enero de 2011 y Twitter en marzo de ese mismo año. Actualmente, los sitios más importantes la utilizan por defecto y es infaltable donde se deban ingresar datos bancarios.**

# 9.
# Cifrado de datos locales

# 9. Cifrado de datos locales

La información que no es transmitida también corre el riesgo de ser accedida por terceros; por ejemplo, ante el extravío o robo de los equipos portátiles. La contraseña de inicio de sesión no es suficiente para proteger los datos, y es allí donde el cifrado entra en juego. En este sentido, puede cifrarse el disco entero, de tal manera que cada vez que se encienda la computadora se deba ingresar la clave para tener acceso a la misma. Este enfoque suele ser el elegido en las empresas, aunque también existe la alternativa de cifrar sólo algunas carpetas o archivos específicos. Además, cabe aclarar que esto se puede extender a cualquier dispositivo que transporte información delicada, como memorias USB.

Otra situación puede ser cuando se ponen datos o servicios a disposición del público. El escenario ideal es aquel en el que cada usuario puede acceder sólo a los datos para los cuales tiene permiso. Desafortunadamente, si existen vulnerabilidades en los servidores de la empresa, las mismas pueden ser explotadas dando acceso a los atacantes a información confidencial. Por ello, la medida de seguridad principal consiste en evitar el acceso indebido, minimizando las vulnerabilidades. Sin embargo, es igual de importante tener un plan de respuesta a incidentes, en caso de que un atacante logre el acceso a datos confidenciales. En esta situación, si se cifran ciertos datos o archivos se reduce la utilidad que obtiene el atacante.
La información de los clientes es sumamente importante y, de no poder garantizar la seguridad de la misma, los clientes dejarán de confiar en la empresa. Un ejemplo de esto se da en el almacenamiento de los datos de autenticación de los usuarios: si las contraseñas se almacenaran en una base sin cifrar, las cuentas de los clientes se verían directamente comprometidas si un atacante lograse acceder a estos registros.

**En julio de 2012 Yahoo! sufrió un ataque donde se robaron alrededor de 500 mil contraseñas de sus usuarios.
Las mismas no se almacenaban cifradas, lo cual permitió el acceso directo a las cuentas comprometidas.***

**Fuente: http://blogs.eset-la.com/laboratorio/2012/07/12/yahoo-nueva-brecha-seguridad-red/*


# 10.

## Cifrado de dispositivos móviles

# 10. Cifrado de dispositivos móviles

Los dispositivos móviles se están convirtiendo en un factor muy importante en las empresas, ya que acompañan a los empleados todo el tiempo y en todo lugar, y brindan acceso inmediato a la información. Debido a que cada vez más información de la empresa puede ser accedida desde un mismo dispositivo, se requiere una gestión adecuada de la seguridad de la información en el mismo.

En primer lugar es importante mencionar que, debido a factores como su tamaño y portabilidad, estos tipos de dispositivos son susceptibles al robo y el extravío, lo que implica un riesgo no menor; el cifrado de los datos almacenados representa, entonces, una medida efectiva contra el acceso no autorizado a la información. Es posible cifrar los datos de las aplicaciones, archivos descargados, fotos, documentos y cualquier otro archivo que sea almacenado en el dispositivo. Así, para lograr acceder a los datos es necesario el ingreso de un PIN o clave, conocida solamente por el dueño del equipo.

También debe considerarse que los dispositivos móviles proveen conectividad con redes que utilizan el aire como medio de transmisión, y donde los datos podrían ser interceptados por terceros que estén dentro del alcance de la señal. Por ello, siempre que se necesite transmitir información sensible resulta fundamental conectarse a una red que envíe la información cifrada entre el dispositivo y el punto de acceso. Adicionalmente, es necesario implementar el cifrado de las comunicaciones que salen a Internet, como los correos electrónicos confidenciales, chats o mensajes instantáneos.

Es posible cifrar los dispositivos móviles con las herramientas nativas del sistema operativo. En Android, por ejemplo, puede encontrarse en **Ajustes/ Seguridad/Encriptar dispositivo.**

Si se interrumpe el proceso, la información podría perderse para siempre, de modo que el dispositivo debe estar conectado a la electricidad y con la batería cargada al máximo. Por lo general, el proceso demora una hora aproximadamente, dependiendo de la cantidad de información almacenada.

# 11.
# Conclusión

# 11. Conclusión

La seguridad en una organización requiere de esfuerzos constantes, que deben acompañarse de inversiones basadas en el valor de la información a proteger, el impacto que tienen en el negocio y en el estado actual de la seguridad en la empresa.

Asimismo, es necesario contar con políticas de seguridad detalladas que identifiquen los activos de información y los riesgos asociados a los mismos, para determinar las posibles acciones preventivas y correctivas. En este contexto, el cifrado de datos es una forma de proteger la información sensible de una organización en todo su espectro: datos almacenados en servidores, comunicaciones e incluso en los dispositivos móviles de sus colaboradores.


ENJOY SAFER
TECHNOLOGY™