ENJOY SAFER TECHNOLOGY™

DEVELANDO LA ESENCIA DEL CIFRADO DE DATOS

DESlock+

La información es uno de los recursos más importantes en una empresa, desde la más pequeña hasta la más grande; de ahí que resulta indispensable protegerla a toda costa.

Una manera de hacerlo es a través del cifrado de datos, una técnica que se utiliza desde hace siglos, siendo el antiguo imperio romano uno de los primeros casos de la historia. El César tenía su código, Da Vinci su Criptex y hasta los alemanes la máquina Enigma durante la Segunda Guerra Mundial...**¿pero cómo es el cifrado en la actualidad? ¿Cómo se usa y qué implica para las empresas?**

¿QUÉ SIGNIFICA CIFRAR LA INFORMACIÓN?

Cifrar datos implica alterarlos, generalmente mediante una clave, por lo que quienes no tengan esa clave no podrán leerlos. De la forma opuesta, quienes sí la tengan, podrán descifrar el proceso y acceder a la información original.

¿POR QUÉ ES NECESARIO HACERLO?

Esta metodología básicamente protege la información de una organización ante varias amenazas, como las infecciones de malware que pueden robar información, así como también contra los accesos indebidos a aplicaciones, bases de datos, servidores o sistemas internos.

En cualquiera de esos casos, si la información efectivamente es robada sería muy difícil para una compañía poder revertir el daño, por lo que es fundamental tomar las medidas necesarias para evitarlo y, si ocurre, contar con la preparación adecuada para minimizar el riesgo, por ejemplo, utilizando datos cifrados.

Entre el **40%** y **50%** de las empresas de la región sufrió una infección con malware durante 2014.

Entre el **30%** y el **45%** de las empresas de la región sufrió un acceso indebido a aplicaciones y/o bases de datos.

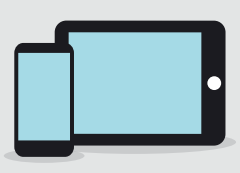
Un **20%** de las empresas de la región aplica controles de cifrado, un **5%** menos que en 2013.

FUENTE: ESET Security Report Latinoamérica 2015:
http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

¿QUÉ INFORMACIÓN ES NECESARIO CIFRAR REALMENTE?

Información que se envía, como correos electrónicos y adjuntos, 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.

Información que no se transmite, pero que está almacenada en dispositivos de la empresa y que salen de la compañía, como computadoras portátiles que pueden ser robadas o extraviadas.



Hardware, como smartphones, tablets, discos y memorias, ya que son cada vez más comunes en el ámbito corporativo, tanto para la transmisión de datos como para el almacenamiento de documentos de trabajo.

¿CUÁLES SON LOS BENEFICIOS?

PROTEGER LA INFORMACIÓN CONFIDENCIAL DE UNA ORGANIZACIÓN

SITUACIÓN

La información sensible de una compañía o de sus clientes cayó en las manos equivocadas por un acceso indebido.

BENEFICIO

Protege frente a perjuicios económicos, de imagen o prestigio; pérdidas de ventaja competitiva; o incluso al cierre de la empresa, ya que no podrían ser leídos sin la clave.

PROTEGER LAS COMUNICACIONES DE UNA ORGANIZACIÓN

SITUACIÓN

Los canales de comunicación por Internet fueron intervenidos por ciberdelincuentes.

BENEFICIO

Protege cualquier tipo de comunicación por vías externas a la compañía, como el correo electrónico, al contar con una clave de cifrado necesaria para leer correctamente los mensajes.

PROTEGER EQUIPOS PORTÁTILES Y DISPOSITIVOS MÓVILES

SITUACIÓN

Un colaborador extravía o le roban un teléfono celular, una tablet o su computadora portátil.

BENEFICIO

Ningún tercero no autorizado y sin la clave podrá acceder a la información cifrada.