Revista Científica Mundo de la Investigación y el Conocimiento

Carlos Arturo Carvajal Chávez [a]

La encriptación de datos empresariales: ventajas y desventajas

The encryption of business data: advantages and disadvantages

Revista Científica Mundo de la Investigación y el Conocimiento. Vol. 3 núm.2, abril, ISSN: 2588-073X, 2019, pp. 980-997

DOI: *10.26820/recimundo/3.(2).abril.2019.980-997*

URL: *http://recimundo.com/index.php/es/article/view/487*

Código UNESCO: 1203.12 Bancos de Datos

Tipo de Investigación: Artículo de Investigación

Editorial Saberes del Conocimiento

Recibido: 15/01/2019 Aceptado: 18/02/2019 Publicado: 30/04/2019

Correspondencia: carvajal@uagraria.edu.ec

a. Magister en Diseño Curricular; Diploma Superior en Diseño Curricular por Competencias; Ingeniero en Sistemas Computacionales; Universidad Agraria del Ecuador; carvajal@uagraria.edu.ec

RESUMEN

La adopción de los avances tecnológicos por parte de las empresas a nivel mundial es un requisito fundamental para lograr sus objetivos. El uso de la tecnología como canal de comunicación, incluso de almacenamiento de información, pone en riesgo la información que por ella transita, de modo que a la par de estos avances también podemos observar el incremento de los delitos informáticos. De allí surge la imperiosa necesidad por parte de las organizaciones de proteger su data digital. En tal sentido, la presente investigación presenta información importante acerca de la encriptación de datos como herramienta de protección para la información de una empresa, el aporte de su adopción contra los riesgos que implican no usarlas y los obstáculos que hasta la fecha presenta esta herramienta. Se desarrolló a traves de una revisión documental de material digital, comparando datos y opiniones encontradas en diferentes sitios web. En conclusión, es fundamental para las empresas adoptar una cultura de encriptación de sus datos, que si bien es cierto que no es la solución total al problema de los delitos informáticos, representa un gran obstáculo para las amenazas que enfrenta.

Palabras Claves: Encriptación; Datos; Empresas; Ventajas; Desventajas.

ABSTRACT

The adoption of technological advances by companies worldwide is a fundamental requirement to achieve their objectives. The use of technology as a channel of communication, even storage of information, puts at risk the information that transits it, so that along with these advances we can also observe the increase in computer crimes. From there arises the urgent need on the part of organizations to protect their digital data. In this sense, this research presents important information about the encryption of data as a protection tool for the information of a company, the contribution of its adoption against the risks that imply not using them and the obstacles that this tool presents up to date. It was developed through a documentary review of digital material, comparing data and opinions found on different websites. In conclusion, it is essential for companies to adopt a culture of encryption of their data, which although it is true that it is not the total solution to the problem of computer crimes, represents a major obstacle to the threats it faces.

Key Words: Encryption; Data; Companies; Advantages; Disadvantages.

Introducción.

Las estrategias en el tan competido mundo empresarial exigen cada día decisiones más acordes a las necesidades cambiantes de los diferentes mercados, en este sentido, uno de los principales bienes de las organizaciones está representado por la información. Los datos de la organización representan la base para la toma de decisiones y su fuga a través de su manejo en la red se traduce en pérdida de dinero, además del prestigio que corre riesgo, sobre todo en aquellas empresas que manejan informaciones importantes de sus clientes.

En este sentido, la solución más viable para la protección de la información empresarial está representada por la encriptación de datos.

> Encriptar es una manera de codificar la información para protegerla frente a terceros. Por lo tanto, la encriptación informática es la codificación de la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red. Es por medio de la encriptación informática como se codifican los datos. Solamente a través de un software de descodificación que conoce el autor de estos documentos encriptados es como se puede volver a decodificar la información. Por lo que la encriptación informática es simplemente la codificación de la información que vamos a enviar a través de la red. La encriptación de la informática se hace cada vez más necesaria debido al aumento de los robos de claves de tarjetas de crédito, número de cuentas corrientes, y en general toda la información que viaja por la red. Todo esto ha fomentado que se quiera conseguir una

mayor seguridad en la transmisión de la información sobre todo a través de Internet. (La Revista Informatica, 2018)

La encriptación de datos ha venido avanzando en la búsqueda de soluciones, el propósito fundamental es desarrollar mejores sistemas que garanticen cada vez más la seguridad de la información, al respecto (Nextvision, 2017) refiere:

> Las soluciones de encriptación como las conocemos en la actualidad se originaron en 1970, con la aparición del algoritmo DES (Data Encryption Standard), desarrollado por el gobierno estadounidense. Se basaba en el cifrado de sustitución por bloques, que consta de transformar un texto de una longitud de bits fija en un texto cifrado de igual longitud, que era de 56 bits. Unos años más tarde, se sustituyó por el Advanced Encryption Standard (AES) un sistema por bloques con claves mucho más seguras, que usan un estándar de 128 bits, pero que pueden llegar a ser de hasta 256 bits. Otro de los algoritmos que actualmente se utilizan es el RSA (Las siglas de Rivest, Shamir y Adleman, sus desarrolladores), que es el que usa el cifrado asimétrico y, a diferencia del algoritmo DES utiliza 2 claves, una pública y otra privada que conserva el propietario del archivo.

> Hoy los datos que residen en los teléfonos móviles están mejor protegidos (más del 80% de datos móviles encriptados) que los datos que residen en la mayoría de centros de datos corporativos (solo se encriptan el 2%). De acuerdo a un estudio de Solitaire Interglobal Ltd., esto sucede porque es más fácil encriptar datos en millones de dispositivos idénticos

> a diferencia de los datos corporativos que son más difíciles y costosos de encriptar, además de que las actuales soluciones de encriptación de datos en ambientes x86, reduce dramáticamente la performance y la experiencia de usuario y puede ser muy compleja y cara de administrar. La epidemia global de violaciones de datos, es un factor importante en el impacto que tendrá el cibercrimen en la economía global hacia 2022. (Marchand, 2017)

En este orden de ideas, (Trott, 2018) refiere que para el 2018 se observa un desinterés de la encriptación de datos empresariales:

> Este debería ser un comportamiento de higiene, percibido como una actividad fundamental. Sin embargo, la adopción del cifrado no ha coincidido con las expectativas de muchos vendedores y comentaristas.

La presente investigación trata de exponer en un compendio el amplio mundo de la encriptación de datos informáticos, con un enfoque hacia la seguridad de la información organizacional y su valoración con respecto a las ventajas y obstáculos que presenta su uso.

Si bien es cierto que existen numerosas investigaciones relacionadas con el área de la encriptación, no es menos cierto que el presente trabajo resume aspectos variados de dicho tema, además de la orientación hacia la relevancia que representa para las empresas su conocimiento y valoración, en pro de la protección de uno de sus bienes más valiosos: la información.

Materiales y Métodos.

El presente estudio se centró en desarrollar aspectos relacionados con la encriptación de datos, definición, tipos, ventajas y desventajas de uso, así como los riesgos que corren las empresas al transitar su información por la red sin el uso de algún tipo de cifrado que la proteja de quienes no desea que accedan a dichos datos, todo ello con la finalidad de plasmar un análisis crítico de qué tan útil pueda ser para las empresas usar este sistema de protección digital.

El desarrollo del presente estudio se realizó a través de una investigación de tipo documental, sustentada por fuentes digitales, las cuales se recabaron a través de motores de búsqueda tales como Google Académico y Google para garantizar el principio de actualidad y veracidad de la fuente. Se revisaron documentos y artículos científicos provenientes de páginas web, y se revisaron opiniones de expertos en la materia, a los fines de comparar los datos recopilados, compendiar y resaltar los de mayor importancia.

Resultados.

Encriptación de Datos

El cifrado es un método para evitar que alguien no pueda tener acceso a información que se desea preservar. Este método consiste en alterar un mensaje antes de transmitirlo, generalmente mediante la utilización de una clave, de modo que su contenido no sea legible para los que no posean dicha clave. De esta forma, cualquier persona que tenga

> acceso al mensaje no podrá entender su contenido a menos que cuente con la clave para descifrarlo. No solo es necesario cifrar, sino hacerlo de manera que la información no sea inteligible ni manipulada por terceros. Sin esta última condición, el cifrado no tendría valor. (AGESIC, 2018)

Por otra parte, (Noriega, 2016) lo define como: "un procedimiento que utiliza los algoritmos correspondientes a la criptografía con el fin de que el mensaje realizado por un emisor, llegue de forma segura a su receptor".

En este orden de ideas, tenemos que el encriptado de datos, requiere un emisor, un canal, en este caso la red (internet) y un receptor, este mensaje es susceptible de que durante su trayecto desde el emisor al receptor sea interceptado por terceros y sea sustraída la información que contiene, lo que crea la necesidad de proteger tal data. La encriptación en palabras sencillas, viene a codificar ese mensaje de forma que sólo quién lo envía y quién lo recibe lo conocen, evitando el riesgo de sustracción por terceros indeseables.

Sistemas de Encriptación

Existen tres sistemas básicos de encriptación, los cuales detallaremos a continuación:

Simétrica

La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad (diciéndola en alto, mandándola por correo electrónico u ordinario o haciendo una llamada telefónica). (Gutiérrez, 2013)

Asimétrica

La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca). (Gutiérrez, 2013)

Híbrida

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento. El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo): Generar una clave pública y otra privada (en el receptor), cifrar un archivo de forma síncrona, el receptor nos envía su clave pública, ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor, enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor). (Gutiérrez, 2013)

Modalidades

> Modalidad de bloques, un método de cifrado en el que el mensaje se divide en bloques y el cifrado se realiza individualmente en cada bloque. Puesto que cada bloque tiene, como mínimo, una longitud de 8 bytes, la modalidad de bloques permite la digna aritmética de 64 bits en el algoritmo de cifrado. Modalidad de secuencia, un método de cifrado en el que se cifra cada byte individualmente. Se considera generalmente una forma de cifrado débil. (IBM, 2013)

Principales riesgos que corre la data digital empresarial

Es importante estar conscientes de los riesgos que corre la información que manejan las empresas, en tal sentido, vamos a exponer los principales riesgos:

Pérdida de datos por robo

> Esto se refiere más a los datos que se están almacenando en los propios hogares. Algunos ladrones se pueden ir directamente a la caja de cartuchos de cinta ligeramente polvorientos en una estantería en la esquina, pero por otra parte, un ladrón experto en tecnología puede detectar rápidamente una pila de unidades de discos duros y pensar que puede revender el hardware por algún valor, antes de haberlo examinado y expoliado. (Espacio Negocios, 2012)

Los empleados curiosos

> Si dejas deliberadamente alguna unidad flash en los aparcamientos de tu empresa. No te sorprendas si muchos de ellos fueron "apropiados" por alguien que pasara por allí y accedieran a las computadoras de tu empresa mediante los datos existentes en la unidad flash. (Espacio Negocios, 2012)

Espionaje industrial

> Siempre existe el riesgo del espionaje industrial. Aunque no es un tema del cual mucha gente de negocios quiera hablar, el hecho es que los competidores hacen espiar a la competencia. (Espacio Negocios, 2012)

Ventajas del uso de encriptado de datos

Múltiples niveles de seguridad

> Los softwares de encriptación pagos hacen uso de los algoritmos de cifrado más avanzados y seguros, como el AES; además, hacen uso de claves de hasta 256 bits, tamaño que se considera ideal por su seguridad y su desempeño al momento de la comunicación. Por último, la gran mayoría de las soluciones sin licencia emplean encriptación simétrica o asimétrica; en cambio, las herramientas pagas utilizan la

encriptación híbrida que, como mencionamos antes, es la más segura y rápida. (Nextvision, 2017)

Administración centralizada

En el caso de las herramientas pagas cuentas con una interfaz de administración centralizada en la que se puede: Definir grupos de encriptación con clave privada, usar containers separados de llave para uso específico, Sincronizar en grupos AD, establecer la fecha de vencimiento de una clave específica para mayor control, hacer uso de mecanismos de recuperación de claves. (Nextvision, 2017)

Cumplimiento de normativas

Hay industrias, como la bancaria, que tienen unos estándares de seguridad en el manejo de la información que deben cumplirse para poder operar. Es fundamental que las empresas cuenten con sistemas de encriptación robustos que garanticen el cifrado de la información según a los estándares nacionales e internacionales. (Nextvision, 2017)

Desventajas del uso de encriptado de datos

Desprotección del usuario final

> La encriptación o cifrado de datos y archivos vuelve ilegibles los datos de cualquier archivo. Es decir, éste será inservible para usuarios no autorizados, pero al mismo tiempo ello supone un riesgo. De hecho, la desprotección de los datos de un archivo reversible resulta obvia, pues contar con la contraseña o los algoritmos permitirá acceder a ellos, aún sin tener autorización. (Power Data, 2016)

Desprotección de los datos críticos

> Los datos confidenciales (sensibles y/o importantes) no tienen una protección especial con este método cuando se produce una violación de archivos encriptados. En estos casos, se corre un importante riesgo económico, pues atenta contra los intereses de la organización, y también de vulneración de normativas de protección de datos. (Power Data, 2016)

Vulnerabilidad antes y después del cifrado

> Como es sabido, crear y recuperar un mensaje cifrado significa contar con un métodos matemáticos de criptografía que denominamos contraseñas o logaritmos. Su objetivo, por lo tanto, es convertir el archivo en irreconocible e incomprensible, pero información no está libre de los riesgos de ataques. Aunque su uso es recomendable para la transmisión segura de archivos, a su vez representa un peligro potencial ante filtraciones, con más probabilidad cuando se tiene acceso al ordenador o a su lugar de almacenamiento, ya sea

en origen o destino, de forma física o no, a través de virus u otro malware. (Power Data, 2016)

Contras del cifrado parcial o total

A la hora de cifrar la información podemos incluir solo los datos críticos o encriptar la totalidad de los archivos. En ningún caso evitamos los inconvenientes. Mientras la encriptación completa es más segura, pues nadie sin la contraseña puede acceder a ellos fácilmente, también nos arriesgamos más a perder los datos en caso de tener problemas técnicos, como el fallo o pérdida de un disco. Ello nos obligará a hacer copias de seguridad con frecuencia. Por otra parte, encriptar de forma selectiva puede suponer un importante riesgo por su misma parcialidad. En este sentido, el enmascaramiento de datos se considera más efectivo (además, dentro de éste puede realizarse una encriptación parcial), sobre todo si buscamos una protección de datos que no sea reversible y al tiempo nos permita trabajar en entornos realistas. (Power Data, 2016)

Menos usabilidad

A diferencia del enmascaramiento, la encriptación no permite trabajar con los datos, pues éstos no ofrecen una visión coherente. Aunque enmascarar significa generar datos ficticios, éstos son realistas y permiten su uso en ambientes productivos, por terceros, en entornos de pruebas, desarrollo o capacitación. Por lo tanto, la encriptación es menos funcional, ya que ofrece una menor usabilidad. (Power Data, 2016)

Recomendaciones para realizar un buen encriptado de datos

El encriptado por sí sólo no es suficiente garantía para la confidencialidad de la información, a continuación, algunas recomendaciones según (Korolov, 2013), para realizar un buen encriptado de datos:

Utilice el cifrado más potente que pueda: si los datos tienen que ser protegidos a toda costa, utilice algoritmos conocidos y probados, además de las claves más largas que pueda gestionar en la práctica. Mantenga sus claves seguras: si la encriptación es tan fuerte que ni siquiera un gobierno extranjero con una supercomputadora puede romperlo, entonces se encontrará con un mundo de problemas si pierde las claves de cifrado. Borre claves para borrar datos en la nube de forma permanente: si su empresa está utilizando la nube para compartir documentos sensibles o para hacer copias de seguridad convenientes, ¿está seguro de que los archivos se han ido realmente al moverlos a la papelera? No guarde las claves junto a los datos: almacenar las claves de cifrado justo al lado de los datos encriptados es como escribir su PIN en su tarjeta de cajero automático, o como dejar las llaves de la caja fuerte en la cerradura.

Otras recomendaciones según (Finanzas Personales, 2017) son: “Analizar a detalle la necesidad del negocio para definir la estrategia de protección de datos. Evaluar distintos productos antes de tomar la decisión final. Usar siempre y en la medida de lo posible algoritmos de cifrado sólidos”.

Conclusiones.

Es innegable que los canales de comunicación informáticos y los diferentes avances tecnológicos facilitan las actividades empresariales, coadyuvan en el cumplimiento de sus objetivos y crean una ventaja sobre sus competidores, no obstante, con el uso de la tecnología han surgido cada vez más los ciberataques o delitos informáticos, los cuales ponen en riesgo, principalmente, la data organizacional.

Las empresas manejan cada vez más datos importantes relacionados propiamente con sus operaciones, pero también datos personales de sus clientes, en este sentido, resulta fundamental protegerlos, a objeto de evitar plagio de estrategias, pérdidas de dinero y en muchos casos pérdida de confianza por parte de sus clientes, este último caso en donde el cliente se ve afectado profundamente, puede ocasionar demandas, pérdidas de dinero y un desprestigio que en muchos casos lleve a la empresa a la quiebra.

En el caso de las empresas bancarias la fuga de los datos de sus clientes puede generar delitos informáticos, que perjudican no sólo a la entidad sino los intereses de sus clientes. Por tal razón, la importancia de la encriptación de los datos empresariales.

Google, Dropbox, Yahoo!, SpiderOak, Twitter y Sonic.net, son algunas de las empresas más reconocidas que han implementado la encriptación en sus servicios on line, de manera que podemos acceder a ellos de forma gratuita.

Sin embargo, a nivel empresarial es importante elegir un sistema de encriptación robusto, acorde con las necesidades propias, que si bien genera un incremento en el gasto de la compañía

se puede ver traducido como inversión al momento de evaluar las ventajas y la principal de ellas, la seguridad digital de sus datos.

En tal sentido, podemos concluir que las ventajas superan con creces los obstáculos que presenta el uso del encriptado, que, si bien es cierto que no es la solución total del problema, representa un gran obstáculo para las personas que la amenaza.

Bibliografía.

AGESIC. (2018). *La importancia en el cifrado de datos.* Montevideo: AGESIC desarollando Uruguay Digital. Recuperado el 06 de Julio de 2018

Espacio Negocios. (06 de Septiembre de 2012). *espacionegocios.com.ar*. Recuperado el 07 de Julio de 2018, de http://espacionegocios.com.ar/para-que-sirve-encriptar-la-informacion-de-la-empresa/

Finanzas Personales. (2017). *Finanzas Personales*. Recuperado el 07 de Julio de 2018, de http://www.finanzaspersonales.co/consumo-inteligente/articulo/como-encriptar-informacion-su-empresa/55647

Gutiérrez, P. (03 de Enero de 2013). *Genbeta:dev*. Recuperado el 07 de Julio de 2018, de https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

IBM. (2013). *IBM® Informix® 12.10.* Canada: IBM Knowledge Center. Recuperado el 07 de Julio de 2018

Korolov, M. (10 de Octubre de 2013). *CIO Perú*. Recuperado el 07 de Julio de 2018, de https://cioperu.pe/articulo/14302/diez-consejos-de-cifrado-para-la-empresa/

La Revista Informatica. (2018). QUE ES LA ENCRIPTACIÓN DE LA INFORMÁTICA. *LaReVinCom, 6*(1). Recuperado el 06 de Julio de 2018

Marchand, P. (17 de Julio de 2017). *IBM*. Recuperado el 06 de Julio de 2018, de https://www.ibm.com/blogs/systems/mx-es/2017/07/la-epidemia-violacion-datos-enormes-implicancias-las-empresas/

Nextvision. (2017). *Todo sobre encriptación de datos para empresas.* Buenos Aires, Argentina: Nextvision. Recuperado el 06 de Julio de 2018

Noriega, S. (2016). *¿Qué es el Cifrado y Para Qué Funciona?: Medida de Seguridad Primordial para tu Empresa.* Ciudad de México: Certsuperior. Recuperado el 07 de Julio de 2018

Power Data. (05 de Febrero de 2016). *powerdata.es*. Recuperado el 07 de julio de 2018, de https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/cinco-inconvenientes-del-encriptado-de-datos

Trott, D. (2018). *Reduce la exaltación de la encriptación de datos empresariales.* Canada: IBM Systems Blog para Latinoamérica. Recuperado el 06 de Julio de 2018