

Seguridad en las tecnologías de información y protección de datos

Luis H. Rivas ¹

Resumen. En la actualidad, muchas organizaciones están migrando sus procesos manuales a procesos automatizados; esto hace que dichas empresas dependan total o parcialmente de las TIC para el correcto funcionamiento de sus actividades, por lo que el uso de éstas, en vez de disminuir crece exageradamente cada día y las empresas que buscan el éxito explotan al máximo estos recursos para la toma de decisiones o para el surgimiento de nuevos mercados. Sin embargo, el problema no es el uso excesivo y el exagerado crecimiento de las TIC, sino más bien, pensar en lo que pueda provocar el mal uso que otros le dan a la información que procesamos y difundimos, al utilizar los recursos electrónicos como Internet, el correo electrónico, las redes sociales, entre otros. Si bien es cierto que las TIC nos facilitan el procesamiento y la transmisión de la información, esto puede traer algunos problemas como la pérdida de privacidad de la misma, ataques cibernéticos y fraude de identidad; este último se está incrementando considerablemente en la actualidad, por lo que se vuelve un problema grave del cual tenemos que estar conscientes y en alerta ante los peligros a que nos exponemos cuando nuestros datos circulan por estos medios electrónicos, sin que existan mecanismos de protección o leyes que rijan el control de dicha información, propiciando de esa manera delitos cibernéticos, tales como la venta de datos personales o el robo de esta misma. Minimizar este problema empieza primeramente por nosotros como usuarios, concientizándonos y tomando los mecanismos necesarios para no exponer nuestros datos personales, crediticios o financieros. Cuidemos nuestros datos, estos son un patrimonio importantísimo que vale oro.

Palabras clave. Seguridad en la información, tecnología de la información, automatización, protección de datos, cibernética, TIC, procesamiento electrónico de datos.

Desarrollo

Este artículo describe la importancia de proteger los datos de las organizaciones, especialmente aquellos generados a través del uso de las Tecnologías de la Información y Comunicación, TIC. Para ello se hace énfasis en el concepto

de TIC, los usos y beneficios de éstas, así como la importancia de la información para las organizaciones. De igual manera, se describe la necesidad de la institucionalización de entes reguladores o protectores del procesamiento de datos.

1. Docente investigador. Escuela de Computación. Escuela Especializada en Ingeniería ITCA-FEPADE. San Miguel. E-mail: luis.rivas@itca.edu.sv



El término Tecnologías de Información (TIC), según lo definido por la Asociación de las Tecnologías de Información de América, por sus siglas en inglés ITAA (Information Technology Association of America), es "el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras". Bajo este concepto, las empresas hoy en día asocian las tecnologías de información con los diferentes sistemas automatizados o de software necesarios para procesar, almacenar, proteger y transmitir la información.

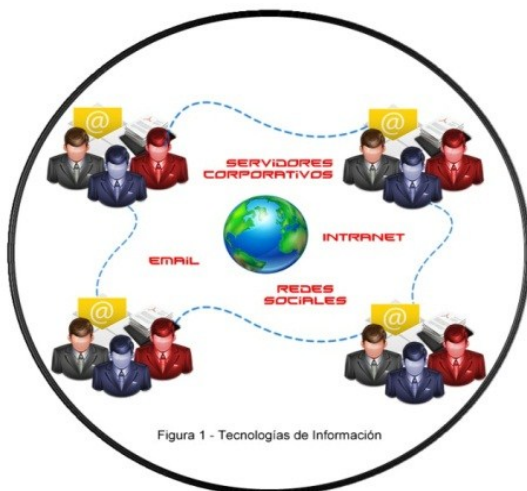


Figura 1. Tecnologías de Información

En un mundo tan globalizado, los datos electrónicos y los medios de comunicación hacen que una organización tenga éxito o fracaso en sus labores, dependiendo de la buena forma o la mala práctica del uso de las TIC. Hablar de tecnologías de información es un campo muy amplio

en donde los profesionales de las TIC deben hacer muchas tareas, desde instalar paquetes de software (como servicios web, servicios de correo, impresión, entre otros), hasta diseñar y configurar redes informáticas de gran complejidad, todo ello para poder mantener la información de la organización protegida y disponible en cualquier momento que el usuario la requiera.

El surgimiento de las tecnologías de información, se puede decir que se inició con el telégrafo, el teléfono, la radiotelefonía, la televisión y hoy en día la Internet, siendo esta última uno de los medios de transmisión más grandes y utilizados en este siglo XXI por las grandes compañías, organizaciones y otros usuarios.

Muchas organizaciones están migrando sus procesos manuales a procesos automatizados; esto hace que dichas empresas dependan total o parcialmente de las TIC para el correcto funcionamiento de sus actividades, por lo que su uso, en vez de disminuir, crece exageradamente cada día y las empresas que buscan el éxito explotan al máximo estos recursos para la toma de decisiones o para el surgimiento de nuevos mercados.

Sin embargo, el problema no es el uso excesivo y el exagerado crecimiento de las TIC, sino más bien pensar en lo que pueda provocar el mal uso o el buen cuidado de la información que procesamos y difundimos utilizando los recursos electrónicos como la Internet, el correo electrónico, las redes sociales, entre otros.

¿Cuán importante es la información que tenemos?

Esta pregunta no debe faltar al momento de utilizar o implementar las TIC en una organización o empresa, y es que hoy en día muchas de éstas usan las TIC para diferentes procesos, desde el intercambio de correos electrónicos, comunicar información a través de un servidor web local (intranet) o público (internet), utilizar un sistema de registro académico, registrar las ventas y compras de la empresa, hasta manipular información financiera o crediticia de las personas. Dado este panorama, independientemente a qué se oriente el uso de las TIC en la empresa, es importante salvaguardar y evitar que personas ajenas manipulen o vean información confidencial.

Si bien es cierto que las TIC nos facilitan el procesamiento y transmisión de la información, esto puede traer algunos problemas tales como:

- **Perder la privacidad de la información:** Cualquier usuario que navegue por Internet puede encontrarse con nuestros datos de forma gratuita y a un bajo costo.
- **Ataques cibernéticos:** Personas mal intencionadas podrían tratar de infiltrarse a nuestra información.
- **Fraude de Identidad:** Con el creciente uso de computadoras también aumenta el número de virus. Éstos buscan a través de códigos maliciosos, no necesariamente dañar los equipos, sino más bien

robar información para fines comerciales, publicitarios o para manipular computadoras.

¿Existen entes reguladores para la protección de datos electrónicos?

Se entiende por dato electrónico aquella información que puede viajar a través de un medio electrónico, capaz de ser leída y procesada por una computadora de forma automatizada.



Figura 2 – Seguridad en Datos

Ejemplo de ello es la información personal de un ciudadano, el record de notas de un estudiante, el estado de cuenta de un cliente, entre otros.

En los países desarrollados, existen entes que velan por la seguridad de los datos que se transfieren a través de Internet; un ejemplo muy claro es la Agencia Española de Protección de Datos (AEPD), la cual es un ente regulador que vela porque la información de carácter personal de sus ciudadanos no sea usada en perjuicio y malversación



de dichas personas o, peor aún, que sea comercializada.

Es por ello que la AEPD, en su artículo 7.2 de la Ley Orgánica 15/1999 dispone que "sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias", prohibiendo el artículo 7.4 "los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual."

¿El Salvador posee una agencia de protección de datos?

En realidad, un ente regulador exclusivamente para la protección de datos electrónicos no existe. Se puede mencionar, por ejemplo, la Superintendencia General de Electricidad y Telecomunicaciones (SIGET), responsable de regular las telecomunicaciones a través de leyes que penalizan procesos incoherentes que velan por los derechos de los usuarios; sin embargo, no cubre de forma completa un área muy importante que es la seguridad e integridad de la información electrónica.

Lamentablemente, la protección de datos es un tema al que en El Salvador no se le ha dado la debida importancia. Hace unos años se dio un incidente en cuanto a la circulación en internet de una base de datos del padrón electoral de las últimas elecciones presidenciales,

con información de cuatro millones quinientos mil salvadoreños (4,500,000), a los cuales también se le sumaron tres millones quinientos mil (3,500,000) datos con información de madre, padre, fecha de nacimiento, dirección de residencia e imagen.

Sin discusión alguna, a partir de esto surgen las preguntas: ¿Cómo se obtuvo esa información? ¿Cuántas personas habrían comprado esa información? ¿No se habrían tomado las medidas de seguridad de los datos? ¿Qué pasaría si esa información hubiese caído en manos de personas con fines lucrativos o delictivos? Se podrían seguir generando más preguntas y la mayoría sin respuestas; pero lo que sí es seguro es que debería de existir un ente regulador y, aún más que eso leyes que castiguen delitos como la posesión y venta de información electrónica de bancos, de datos públicos y privados, así como también leyes que eviten la comercialización de datos personales.

El desafío y reto está frente a nuestros ojos y, como usuarios o profesionales de las TIC debemos considerar el riesgo que corremos al poner nuestra información a nivel público. Es por ello que buscar los mecanismos adecuados de seguridad es un reto para los administradores de las TIC y, más aún, para las personas que usan estas tecnologías para el desarrollo de sus actividades.

Para finalizar, es necesario recordar que nuestra información es oro... ¡¡cuidémosla!!

Recomendaciones

Algunas recomendaciones para evitar problemas de seguridad con el uso de las TIC y la forma de distribución de éstas, se pueden mencionar las siguientes:

- ❖ Evite abrir archivos adjuntos de dudosa procedencia en correos electrónicos.
- ❖ No revele sus datos personales: contraseñas, números de tarjetas de crédito, cuentas de usuario.
- ❖ Utilice contraseñas seguras, combine mayúsculas, minúsculas y números.
- ❖ Cambie cada cierto tiempo la contraseña.
- ❖ Tenga instalado un antivirus confiable.
- ❖ Los profesionales de las TIC deben habilitar proxies, firewall o políticas de acceso en sus redes de datos.
- ❖ Mantenga su sistema operativo actualizado.
- ❖ Si usa una computadora pública, no utilice servicios de pagos en línea o cualquier transacción electrónica.
- ❖ Las redes inalámbricas abiertas son un riesgo, ya que otros usuarios podrían filtrar nuestros datos.

Bibliografía consultada

1. Gómez Vieites, A. 2007. Enciclopedia en la seguridad Informática. México, D.F., Alfaomega. 664 p.
- Puentes Calvo, JF. 2009. Principios de seguridad en el comercio electrónico. México, D.F. Alfaomega. 256 p.
 Disponible en <http://www.agpd.es/portalwebAGPD/canalciudadano/>
 Disponible en http://www.prensalibre.com/noticias/justicia/Corte-salvadorena-Infornet-vender-permiso_0_438556297.html
 Disponible en <http://www.csj.gob.sv/Doctrina.nsf/c5bbb727e7b3b30d06256d48005ecf9c/51aeb2ee4d>
 Disponible en http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=8613&idArt=2663667
 Disponible en http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6358&idArt=5400572