UNA NECESIDAD EN LAS EMPRESAS: LA CIBERSEGURIDAD

[2]Raúl Manuel Arano Chávez
Jesús Escudero Macluf *
Luis Alberto Delfín Beltrán *

INTRODUCCIÓN

Con el uso de las tecnologías en las empresas se les facilitan tener un acercamiento con sus clientes de forma global a través de un correo electrónico donde se les envíe por ejemplo un catálogo de productos, felicitaciones de cumpleaños, un boletín de noticias, o muchos otros servicios más, sin que esto le represente un costo adicional. De la misma forma con la creación de un portal web donde podremos representar nuestra marca, servicios, productos y que nuestros clientes puedan realizar sus compras en línea en cualquier día de la semana en cualquier horario.

Es por ello, que una empresa al menos debe contar con un portal web, correo electrónico, un sistema de gestión de clientes y estar en permanente comunicación a través de las redes sociales, para conocer los valores que debe agregar a su producto y/o servicio con respecto a las características que sus clientes prefieren.

Una nueva forma de hacer negocio es el Comercio Electrónico, quien ha tenido gran relevancia en la actividad de una empresa ya que han tenido que incorporar herramientas para las transacciones bancarias o pagos en línea, así como la generación

* * Investigadores del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas de la Universidad Veracruzana. Correo electrónico: rarano@uv.mx, jescudero@uv.mx y ldelfin@uv.mx

de facturas electrónicas que demanda tener una infraestructura local o tercerizar el servicio.

En este sentido, cobra mayor impacto la seguridad en las tecnologías de la información y comunicación de una empresa, ya que al utilizar la internet como medio de comunicación interna y externa, en este mundo globalizado están expuestos a las amenazas de seguridad de su información.

Los objetivos de los "ciberdelincuentes" no solo se ven reflejados en ataques a empresas grandes o también basan sus ataques en pequeñas y medianas empresas, por lo que toda empresa sin importar su "sector" y/o tamaño deben poner mayor cuidado en la seguridad de sus datos, quizá lo más importante en las empresas no sea solo el cliente sino toda la información que genera el cliente.

LAS TECNOLOGÍAS DE LA INFORMACIÓN INCLUSTADAS EN LAS EMPRESAS.

El uso de las Tecnologías de la Información y Comunicación (TIC´s), en las empresas se ha vuelto en algo imprescindible en toda su estructura organizacional, tomándolas como herramientas tecnológicas que optimizan y mejoran sus procesos administrativos-operativos, agilizando sus operaciones administrativas, de toma de decisiones, procesamiento de datos y en el análisis de información.

Con el uso de la internet como aceleradora de procesos las empresas tienen que cambiar sus estrategias de trabajo al interior como al exterior y a continuación presentaremos las que desde nuestro opinión son más utilizadas por las empresas:

1) Internet en la nube (Cloud Computing)

Fernández morales en su libro "Computación en la nube para automatizar dice que **"**De acuerdo con Ioni y Ioni (2011), en la

actualidad, la mayoría de la infraestructura de computación en la nube se compone de servicios confiables a través de puntos llamados "centros de datos" y construidos en los servidores con varios niveles de tecnologías de virtualización. Los servicios son accesibles en cualquier lugar y permiten el acceso a la infraestructura de redes. Esta forma de acceso satisface todas las necesidades i**nformáticas de los consumidores".** (Fernández Morales, 2012)

2) Comercio Electrónico (E-Commerce)

La Procuraduría Federal del consumidor en su portal electrónico lo precisa como: *"El proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación."*

"Representa una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo. Las compras de artículos y servicios por internet o en línea pueden resultar atractivas por la facilidad para realizarlas, sin embargo, es importante que los ciberconsumidores tomen precauciones para evitar ser víctimas de prácticas comerciales fraudulentas" (PROFECO, 2016).

Este modelo de negocio electrónico garantiza a las empresas capacidad en la oferta de sus servicio y/o productos, bajo costo de operación, procesos comerciales agiles y eficientes, ingreso al mercado global, utilización de nuevas tecnologías y calidad en el servicio. Aunque no asegura el éxito puede ser un gran canal de distribución en las empresas.

3) Negocio Electrónico (E-Bussines).

Jorge Eliécer Prieto Herrera, en su libro "Investigación de Mercados" lo define como *"actividad o proyecto empresarial que tiene como escenario la utilización de un medio electrónico". (Prieto Herrera, 2009).*

Logra una mejor integración entre el proveedor-cliente, disminuye los costos de operación, integra un mejor conocimiento del mercado y permite entrar al mundo globalizado.

4) Big Data

De acuerdo con el análisis realizado por el AMIPCI (Asociación Mexicana de Internet) el término Big Data se refiere a "la acumulación masiva de datos. Esta tendencia se enmarca principalmente en actividades relacionadas con sistemas que manipulan grandes conjuntos de datos, que supera la capacidad de sistemas tradicionales para ser capturados, gestionados y procesados en un tiempo razonable" (AMIPCI, 2015).

La manipulación de grandes cantidades de datos personales se centra en un proceso de captura, almacenamiento, análisis, y visualización. La captura u obtención de los datos se pueden realizar a partir de diversos mecanismos, ya sean los generados por las personas, transacciones de datos, mecanismos de e-marketing y páginas Web.

El almacenamiento se realiza mediante plataformas o sistemas para extraer, homologar y generar bases de datos; el análisis que se puede realizar mediante asociaciones, análisis de textos, minería de datos (Data Mining) referida al análisis de comportamientos predictivos, o Clustering de datos, mediante la agrupación de grupos pequeños de individuos para identificar comportamientos similares; y su visualización a través de imágenes, gráficas, infografías, entre otros.

Este concepto se puede ser utilizado en una gran variedad de ámbitos, como el desarrollo de campañas de comercialización específicas para perfiles de usuarios de redes sociales; venta de nuevos productos y servicios basado en patrones de compra de usuarios, creando anuncios personalizados y boletines electrónicos.

En este sentido, representa grandes oportunidades para el desarrollo y crecimiento de nuevos negocios basados en datos personales, pero también comporta importantes riesgos. Por lo que las empresas deben ser cautas con los riesgos asociados a sus procesos de captura, identificación, re-identificación, análisis predictivo y recolección de información, concediendo especial atención en el tratamiento de datos de carácter personal.

5) Mercadotecnia Electrónica (E-Marketing)

La mercadotecnia en el internet es la posibilidad de promocionar y difundir los productos y/o servicios de forma global a través de la red de redes, mostrando como ventajas el contacto directo con los potenciales clientes, realizar campañas masivas a todos los usuarios del internet, innovación en la penetración de los productos ante los clientes y el ingreso al mercado global a bajo costo.

"La comunicación es importante para darnos a conocer y que conozcan nuestras intenciones, pero para generar resultados a lo largo del tiempo usted necesita tener acción permanente. Esta acción debe estar respaldada por una estrategia corporativa y ambos tipos de estrategias (corporativas y sectoriales) responden a la visión que usted se proponga. (Moncalvo, 2016)

LOS RIESGOS CIBERNÉTICOS EN UNA EMPRESA.

Como hemos visto las bondades que ofrecen las Tecnologías de la Información y Comunicación (TIC´s) a las empresas, estas han permitido que este sea un gran sector de oportunidades para todos aquellos que desean comercializar o difundir sus productos, pero esto ha llevado a que se tenga que reglamentar el uso de estas para no caer en "dificultades técnicas".

Pero esto también nos ha traído que personas ajenas quieran lucrar con nuestra información y sea una amenaza constante en el día a día de nuestros procesos informáticos.

La protección de los datos no ha sido bien valorada en México, sobre todo en las pequeñas y medianas empresas, creyendo que estas no son un objetivo importante para los "hackers", recordemos que estos "personajes" navegan todo el tiempo en la red en busca de sitios vulnerables y al encontrarlos no dudan en mostrar sus habilidades para sustraer su información.

Recordemos que un gran porcentaje de negocios se apoyan en bases de datos con conexiones remotas, software de gestión y el uso continuo de Internet, por lo que tener en tu empresa un posible fallo o deficiencia en la seguridad de tus "servidores" o equipo de telecomunicaciones representa un grave problema que puede significar la pérdida de datos importantes, afectando gravemente el desempeño y seguridad.

Como las amenazas más comunes encontramos las siguientes:

a) Phishing

De acuerdo a la publicación que realiza el portal web Panda Security el "phishing" consiste en "*el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.*

Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador". (Secutity, 2016)

b) Ataques de fuerza bruta

Ataque por fuerza bruta es el método que se utiliza para averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Los ataques por fuerza bruta son una de las técnicas más habituales de robo de contraseñas en Internet dado que no es necesario tener grandes conocimientos en seguridad informática para realizar uno y existen programas que realizan de forma automática esta labor. http://faqoff.es/que-es-un-ataque-por-fuerza-bruta/

c) Robo de identidad

La CONDUSEF en su revista "Proteja su dinero" lo describe "Cuando una persona obtiene, transfiere, posee o utiliza de manera no autorizada datos personales de alguien más, con la intención de asumir de manera apócrifa su identidad y realizar compras, obtener créditos, documentos o cualquier otro beneficio financiero en detrimento de sus finanzas.

Tu identidad la constituyen datos personales como: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y seguridad social, números de tarjeta de crédito y cuentas bancarias, nombres de usuario y contraseñas." (CONDUSEF, 2016)

d) Ataques de negación de servicios (DoS)

Se entiende como que una persona "ajena" se apropie de un recurso o servicio de una empresa con la intención de evitar cualquier acceso de sus clientes. También, se incluyen los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

e) Spyware o Keylogger

Software o hardware instalado en una computadora, generalmente sin el conocimiento del usuario, que recoge información de dicho usuario para más tarde enviarla por Internet a un servidor remoto.
http://www.internetglosario.com/828/spyware.html

f) Hackeo

Un hacker es aquella persona experta en alguna rama de las TIC´s, dedicado a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

http://cristianargelvergara.blogspot.mx/p/inicio.html

La palabra hacker es tanto un neologismo como un anglicismo. Proviene del inglés y tiene que ver con el verbo "hack" que significa "recortar", "alterar". A menudo los hackers se reconocen como tales y llaman a sus obras "hackeo" o "hackear".

http://www.definicionabc.com/tecnologia/hacker-2.php

CONCLUSIONES

Las empresas hoy en día requieren de establecer mayores medidas de seguridad en su infraestructura de las Tecnologías de la Información y Comunicación, y deben de contratar a personal especializado en seguridad ya sea interna y/o externa que le permita contar con un plan definido para prevenir o mitigar los posibles ataques que pudiera tener, no olvidemos que por el simple hecho de que las empresas utilicen sistemas de información o servicios de internet son vulnerables a todo tipo de ataque sin importar el tamaño de la empresa.

De suma importancia establecer en la organización políticas de seguridad con respecto a: utilización de antivirus corporativo y licenciado, disminuir los tiempos de navegación en la web de sus empleados, evitar la descarga de archivos desde sitios no legales, filtrar los correos electrónicos de dudosa procedencia y crear perfiles laborales con acceso restringido de información y sobre todo estar siempre alertas a que así como la tecnología en las empresas evoluciona, de la misma forma las medidas de seguridad deben de ser cada vez más complejos.

REFERENCIAS BIBLIOGRÁFICAS

AMIPCI. (2015). *ESTUDIO SOBRE EL VALOR ECONÓMICO DE LOS DATOS PERSONALES*. AMIPCI.

CONDUSEF. (12 de OCTUBRE de 2016). *CONDUSEF*. Obtenido de http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad

Fernández Morales, M. (2012). *Computación en la nube para automatizar unidades de información*. Red Universidad Nacional de Costa Rica.

Moncalvo, A. (2016). *Comercio Electrónico para Pymes*. Buenos Aires: Ugerman.

Prieto Herrera, J. E. (2009). *Investigación de Mercados*. Ecoe Ediciones.

PROFECO, P. F. (2016). *Profeco / Secretaría de Economía*. Recuperado el miércoles 12 de Octubre de 2016, de http://profeco.gob.mx/internacionales/com_elec.asp

Secutity, P. (12 de octubre de 2016). *Panda*. Recuperado el 12 de octubre de 2016, de http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

CONSULTAS WEB

Aprendizaje Educativo del Desarrollo de las TIC. Obtenido de http://cristianargelvergara.blogspot.mx/p/inicio.html. (Consultado el 21 de octubre de 2016)

Definición ABC. Obtenido de http://www.definicionabc.com/tecnologia/hacker-2.php. (Consultado el 21 de octubre de 2016)

Glosario de I nformática e Internet. Obtenido de http://www.internetglosario.com/letra-s.html. (Consultado el 21 de octubre de 2016)
Consejos de seguridad para Pymes. Obtenido de http://www.all4sec.es/blog/consejos-de-seguridad-para-pymes/. (Consultado el 21 de octubre de 2016)
¿Qué es el Internet marketing? Obtenido de http://www.internet-marketing.es/que-es-internet-marketing.html. (Consultado el 21 de octubre de 2016)