REVISTA CARIBEÑA DE CIENCIAS SOCIALES
Febrero 2016 - ISSN: 2254-7630

PROPUESTA PARA MITIGAR EL RIESGO DE VULNERABLE EN LOS PROYECTOS INFORMÁTICOS DE UNA ORGANIZACIÓN

Orellana Intriago Fernando MSc.

Facultad de Ciencias Administrativas Cdla Universitaria Salvador allende Universidad de Guayaquil presimaster1@hotmail.com Docente en la Cátedra de Procesos Administrativos.

Cordova Aragundi Jose Saturdino MSc.

Facultad de Ciencias Administrativas Cdla Universitaria Salvador allende Universidad de Guayaquil jscordovaa@hotmail.com Docente en la Cátedra de sistemas informáticos y programación.

Carrasco Cachinelli Carlos MSc.

Facultad de Ciencias Administrativas Cdla Universitaria Salvador allende Universidad de Guayaquil ccarrasco21@hotmail.com Docente en la Cátedra de sistemas informáticos y programación.

Mata López Daniel Antonio MSc.

Facultad de Ciencias Administrativas Cdla Universitaria Salvador allende Universidad de Guayaquil danielmata_79@hotmail.com Docente en la Cátedra de sistemas informáticos y programación.

RESUMEN

La Tecnología de Información ha evolucionado de manera acelerada en el mundo actual, pero a su vez también se han incrementado los riesgos y vulnerabilidades a las que están expuestas las diferentes organizaciones, por lo cual la seguridad de la información se ha vuelto un componente clave en el éxito o fracaso de una organización al momento de enfrentarse a la competencia.

El presente documento de investigación expone una propuesta para mitigar el riesgo de vulnerabilidades en los proyectos informáticos de una determinada empresa, se presentan recomendaciones tanto a usuarios como a personal del área de sistemas para prevenir y cuidar la información tanto personal como institucional, y de esta manera obtener una mayor productividad y competitividad en el mercado sobre el cual se desenvuelve.

Palabras Claves

Mitigar, vulnerabilidades, seguridad, información, competitividad, productividad.

SUMMARY

Actually, Information Technology has evolved at an accelerated way , but at the same time have also increased the risks and vulnerabilities that are exposed to different organizations, so the information security has become a key component in the success or failure of an organization when facing competition. This investigation presents a proposal to mitigate the risk of vulnerabilities in IT projects of a certain company, recommendations are presented to both users and professionals in the area of prevention and care systems for both personal and institutional information, and this so higher productivity and competitiveness in the market on which it operates.

INTRODUCCION

Las actividades dentro de una organización hoy en día tienen una mayor dependencia de las Tecnologías de la Información (TI). Esto obedece a la rapidez con la que va evolucionando el mundo moderno que cada vez es más exigente de conocimientos, habilidades y nuevos desafíos tecnológicos, “Desde sus inicios, la tecnología ha estado en constante evolución, y

la velocidad con la que esto ocurre es casi increíble" (Hawking, 2004). De información tomadas de la encuesta y actividades de ciencia, tecnología e innovación (INEC, 2009 - 2011) realizado por el INEC[1], El 54,4% de las personas que usan Internet lo hacen por lo menos 1 vez al día, mientras el 39,5% lo hace por lo menos 1 vez a la semana.

Del mismo modo como ha avanzado la tecnología, se han incrementado también las amenazas de las cuales podemos ser objetos quienes utilizamos dicha tecnología tanto los usuarios comunes como las organizaciones en general, motivo por el cual la seguridad informática se ha vuelto cada vez más importante en la vida cotidiana e institucional, "La seguridad Informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable" (Aguilera López, 2010)

Por lo tanto y teniendo en cuenta diferentes escenarios tales como: el entorno actual de tecnología, el aumento de delitos informáticos, el establecimiento de normas y estándares de informáticos, y el enfoque de posicionar a la Organización entre las mejores del país y el mundo, implementaremos un instructivo en el que se dé a conocer entre los integrantes del área de tecnología de la información de una organización las diferentes recomendaciones, normas y estándares de seguridad informática, mediante el cual se pueda minimizar el riesgo de vulnerabilidades en los proyectos informáticos de una organización tanto los actuales como los se implementarán posteriormente.

Finalmente, con el presente documento se analizará el cumplimiento del objetivo propuesto y su aporte en la organización, el mismo que nos va a permitir mitigar el riesgo de vulnerabilidades en los proyectos informáticos y su vez aumentar el desempeño de la Organización, en términos de eficiencia, eficacia, relevancia y competitividad.

[1] INEC – Instituto Nacional de Estadísticas y Censos - http://www.ecuadorencifras.gob.ec/

MARCO TEÓRICO

SEGURIDAD INFORMÁTICA

La Seguridad de la Información es la disciplina que se encarga del análisis de riesgos, amenazas, planes de acción de buenas prácticas y normativas para el aseguramiento de procesos y tecnologías. Por otra parte, la Seguridad Informática es la parte táctica y operacional de la Seguridad de la Información, que implementa las técnicas de protección sobre los activos (Cano, 2011)

La finalidad de la seguridad es permitir que una organización cumpla con todos sus objetivos (Areitio, 2008) implementando sistemas de TI en especial consideración para todas las partes involucradas (clientes, socios, administradores, etc). (Royer, 2004), identifica la seguridad del sistema como la protección contra cada una de las amenazas potenciales, siendo estas las principales aunque no las únicas: el pirateo, la cual consiste en el acceso no autorizado de un tercero al sistemas de información de la empresa; los virus, trata de programas maliciosos que generalmente se reproducen de manera autónoma, ya sea a través de Internet, del correo electrónico o de los diversos dispositivos de conexión al sistema de información, es de las amenazas más frecuentes; otra amenaza consiste en la intercepción de datos confidenciales, la cual trata de un tercero que consigue obtener de manera indebida datos o documentos que utiliza la empresa, aunque no sea precisamente para dañar al sistema de información; y la denegación del servicio, la cual trata de estropear algunos componentes estratégicos como el servidor, el correo, la página web, etc.

El activo más importante de las organizaciones es la información con que se trabaja, ya que prácticamente es la esencia de la herramienta y por ende necesita estar protegida (Areitio, 2008); esto se logra implementando una serie de controles: políticas, procesos y procedimientos que se necesitan establecer, implementar, monitorear, revisar y mejorar estos mismos para asegurarse que cumplan con los objetivos de la seguridad.

La falta de seguridad de los sistemas de información ha incrementado la oportunidad para la manipulación, falsificación o alteración de los registros contables (Wen&Beard, 2007),

es por ello que los profesionistas en esta área deben estar conscientes de las amenazas a la seguridad de las computadoras a fin de protegerlas, a sus aplicaciones, a la información de clientes y la de la propia organización (Davis, 1997), porque se ha determinado que es preciso reforzar los controles de seguridad en los sistemas de información, y que muchas empresas empiezan a usar Tecnologías de la Información sin estar protegidos correctamente, para lo que (Gundavelli, 2001) propone tres elementos para la seguridad de datos financieros:

Autenticación: limitar el acceso sólo a las personas indicadas.

Autorización: proveer el control de acceso sólo a personas que pueden hacer cambios en la información.

Confidencialidad: encriptar / desencriptar la información a las personas correctas.

Dentro de los principales controles internos destacan: el acceso físico, acceso lógico, medios de almacenamiento, procedimientos, respaldos de información, captura de datos, accidentes de trabajo (destrucción de información), virus computacionales, desastres naturales o provocados por el hombre, compartición entre empleados de passwords, impresiones perdidas, distribución de información a personas no autorizadas, entre otros.

Sin margen a equivocarse, principalmente los profesionales de la contaduría (como usuarios, directivos, diseñadores y evaluadores de los sistemas de información) deberían tener el conocimiento de las amenazas a la seguridad y de las técnicas apropiadas de control a fin de proteger sus SIC (Wen&Beard, 2007), que les permita contar en el corto plazo con esa eficiencia en el desempeño organizacional y a la vez enfrentar con mayor confianza a la competencia regional, nacional e internacional.

Toda organización debe estar a la vanguardia de los procesos de cambio donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental donde tener información es tener poder donde la información se reconoce como:

Crítica, indispensable para garantizar la continuidad operativa de la organización es un activo corporativo que tiene valor en sí mismo que debe ser conocida por las personas que necesitan los datos

La medida principal frente a las amenazas, debe ser de carácter preventivo, para preservar la confidencialidad a considerar en la concepción y desarrollo del sistema, es el diseño del control de accesos lógicos en su diseño se deben de tener en cuenta las siguientes consideraciones.

Establecer los grupos de usuarios por niveles de seguridad, asignando a cada uno, los tipos de accesos permitidos lectura, modificación, tratamientos, periféricos

El acceso lógico al entorno corporativo se realiza bajo el control del producto por lo tanto es preciso diseñar los controles Posibles grupos a considerar y las medidas de auditoría a implementar para la inclusión del sistema.

METODOS

Implementación de métodos de protección de información

Realizar evaluaciones de vulnerabilidades web para complementar la protección de datos con el análisis y escaneo automático, y de manera periódica, de vulnerabilidades en aplicaciones web, así como en el *software* (sistema operativo) del servidor y los puertos de red. Se deben examinar todos los puntos de entrada que son los más utilizados para ataques comunes. Para realizar una óptima evaluación la podemos dividir en tres fases:

Con el análisis se detectan la vulnerabilidades más comunes (*cross-site scripting*, inyecciones SQL…), incluyendo los programas y software obsoletos o sin sus últimas actualizaciones (parches), y las puertas traseras.

Una vez realizado el análisis, la evaluación debe ofrecer un informe con los datos obtenidos para facilitar el trabajo del departamento de tecnología y mitigar las vulnerabilidades encontradas. Así se aumenta la visibilidad sobre la seguridad para los responsables de las telecomunicaciones de la organización.

Finalmente es aconsejable que el sistema haga un repaso a las páginas y aplicaciones web analizadas para comprobar que las vulnerabilidades se han solucionado.

Lo ideal para complementar la evaluación y minimizar los riesgos de las vulnerabilidades web es la implementación de un *firewall* con control de aplicaciones (*Web Application Firewall*).

Un cortafuego que realiza el seguimiento de las páginas y sistemas web que sea capaz de bloquear la entrada y salida de las solicitudes de acceso al sistema que no cumplan con las configuraciones de vulnerabilidades y amenazas en sitios web definidas en este equipo. De esta manera el *firewall* protege el servidor web más allá del cortafuego de red tradicional.

Realizar una reducción de ataques gracias a una óptima evaluación de vulnerabilidades web

El comercio **y** los negocios online la primera norma para mantener al cliente satisfecho es garantizar la seguridad de sus datos y transacciones *online***,** cumpliendo con las regulaciones en materia de protección de datos. Y en un horizonte siempre cambiante de amenazas y soluciones es imprescindible una protección dinámica.

Con el fin de no tener que pagar con la reputación de la empresa, los valores derivados de una multa por transgredir el cumplimiento de normativas o el descenso de los ingresos al resultar “sospechosos” a los clientes, es fundamental conservar a raya las vulnerabilidades

de páginas y aplicaciones web y no permitir que ingresen y se acumulen en nuestro servidor web.

Una evaluación apropiada y simplificada de las vulnerabilidades web, en combinación con un *firewall* con control de aplicaciones, reducirá el valor del conjunto de la gestión de vulnerabilidades web haciéndola mucho más sencilla y eficiente. Una mayor transparencia y claridad de estos procesos facilitará las tareas de seguridad y protección de datos del departamento de tecnología reforzando la capacidad de la organización en esta materia.

EXPERIMENTO

DIFERENTES AMENAZAS EN SEGURIDAD INFORMÁTICA

El usuario que consciente o inconscientemente causa un inconveniente o problema de seguridad informática.

Programas o software maliciosos tales como virus, troyanos, programas espía, etc.

Un intruso que consigue acceder a los datos o programas a los cuales no tiene acceso permitido.

Un incidente, como una inundación, un incendio o un robo que provocan la pérdida de equipos o información.

TIPOS DE AMENAZA

AMENAZAS LÓGICAS

Intencionadas virus malware uso de herramientas acceso no autorizado software incorrecto provienen de errores cometidos de forma involuntaria por programas.

Los protocolos de comunicación que son utilizados en su mayoría carecen de seguridad o esta ha sido implementada en forma de parche tiempo después de su creación.

Existen agujeros de seguridad en los sistemas operativos, las aplicaciones, errores en las configuraciones de los sistemas, etc.

Las organizaciones en muchas ocasiones no denuncian los ataques a sus sistemas, pues esto ocasionaría que baje el nivel de confianza de los clientes.

Los Administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

AMENAZAS FÍSICAS

Estas amenazas pueden ocasionarse por muchos factores:

Fallos en los dispositivos. Pueden fallar los discos, el cableado, la suministro de energía, etc., provocando una caída en los equipos informáticos o en los sistemas, Catástrofes naturales (terremotos, inundaciones, etc.).

Tradicionalmente los virus han sido uno de los principales riesgos de seguridad para los sistemas informáticos. El principal método de propagación es a través de las redes informáticas e Internet, reproduciéndose e infectando equipos conectados.

Fallos en los dispositivos catástrofes naturales terremotos.

COMO APLICAR LA SEGURIDAD INFORMÁTICA

Generalmente la seguridad se concreta en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos solo poseen los derechos que se les han otorgado. La seguridad Informática deber garantizar: La Disponibilidad de los sistemas de información, la recuperación rápido y completo de los sistemas de información, la Integridad de la información, la confidencialidad de la información.

DISCUSION.

Según un estudio de Symantec (symantec, 2011), existen decenas de miles de vulnerabilidades conocidas, y este número crece exponencialmente año a año. Un acrecentamiento facilitado por el auge de los *scripts* automatizados y los kits de herramientas de ataque web. Estos paquetes de software *malware* están creados específicamente para aprovechar las vulnerabilidades web y facilitar el lanzamiento de ataques generalizados.

De esta manera surgen nuevas necesidades de seguridad, de funciones más ágiles, simplificadas y automatizadas que permitan a los administradores web ser capaces de identificar a tiempo las vulnerabilidades y corregirlas o parchearlas antes de que se conviertan en amenazas y ataques que deriven en el robo y manipulación de información sensible de recursos humanos, clientes o finanzas.

Los delincuentes informáticos, siempre está dispuesta para aprovechar los fallos comunes de *software* y las vulnerabilidades creadas a partir de un dispositivo o configuración de equipos de seguridad inadecuados. Y muchas organizaciones no disponen de los recursos necesarios o el personal indicado para "taponar" esas vulnerabilidades o hacer frente a sus amenazas.

Los ataques más peligrosos y los que de manera más rápido se están extendiendo, según el informe de Symantec, son los automatizados, los dirigidos.

Prácticas maliciosas como las inyecciones SQL, que permiten a los delincuentes informáticos acceder a las bases de datos corporativas; o *cross-site scripting* (XSS), que les permite agregar código malicioso al sitio web para ejecutar tareas, muy típico en aplicaciones web como las tiendas *online*.

Estos métodos pueden dar a los atacantes el control de la aplicación web facilitándoles así el acceso a servidores, motores de bases de datos y otros recursos de las telecomunicaciones corporativas. Una vez que han accedido a estos pueden obtener números de tarjetas de crédito, información privada de empleados y otros datos críticos.

CONCLUSIONES

Con esta investigación se pretende fortalecer en los conocimientos de prevención ante los posibles ataques tecnológicos y a su vez dar el debido valor a las seguridades de la información dentro de una organización y demostrar el grado de influencia que tiene la seguridad informática y la administración de la información respecto a la competitividad y

productividad en la organización; ya que la mayoría piensa que tener un buen antivirus y contar con algún tipo de equipamiento en seguridad se encuentran exentos de un ataque o robo de información, y esto no es así, ya que se deben de tomar en cuenta muchos factores pero sobre todo contar con implementación de métodos de seguridad para la prevención de vulnerabilidades y protección de la información; como se indica en la propuesta/discusión y análisis, no hay que olvidar que la información es considerada como un activo para la organización, por lo que no debe quedar expuesta a un ataque.

Este documento propone una constante revisión de los procesos de implementación de sistemas, capacitación a los usuarios para la prevención de ataques futuros, y esta manera buscar un fortalecimiento institucional y una mayor protección de la información de la organización.

BIBLIOGRAFIA.

Aguilera López, P. (2010). Seguridad informática. En P. Aguilera López, *Seguridad informática* (pág. 9).

Areitio. (2008). Seguridad de la información. Redes, Informática y Sistemas de Información. En Areitio. Paraninfo.

Cano. (2011). La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes. *ISACA* .

Davis. (1997). An Assessment of Accounting Information Security. En Davis.

Fiscalía_General_Ecuador. (2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Recuperado el 2015, de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Gee. (2014). Cyber Security Principles.

Gundavelli. (2001). Security in Web-Based Finance. Business Credit. En Gundavelli.

Hawking, S. (2004). Brevísima historia del tiempo. En S. Hawking, *Brevísima historia del tiemp* (pág. pág. 17). EU.

Hernández. (2009). El Delito Informático. EGUZKILORE.

INEC. (2009 - 2011). *Encuesta de Actividades de Ciencia, Tecnología e Innovación*. Recuperado el 2009 - 2011, de http://www.ecuadorencifras.gob.ec/ciencia-tecnologia-e-innovacion/

J, A. (2008). Seguridad de la información. Redes, Informática y Sistemas de Información. En A. J. Paraninfo.

Medina&Rico. (2011). Mejores Prácticas de Gestión para la Calidad de los Servicios en Tecnologías de Información. En Medina&Rico.

Montenegro. (2015). *Seguridad de la Información: Más que una actitud, un estilo de vida*. Obtenido de http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

Royer, J. (2004). Seguridad en la informática de empresa: riesgos, amenazas, prevención y soluciones. En J. Royer. Ediciones ENI.

Santos, C. (2014). *Seguridad informática.* Madrid: RA-MA Editorial.

symantec. (2011). *Reducing the Cost and Complexity of Web Vulnerability Management.* Symantec.

Wen&Beard. (2007). Reducing the Threat Levels for Accounting Information Systems. En Wen&Beard.