UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

http://revistas.udistrital.edu.co/ojs/index.php/vinculos

Revista VÍNCULOS
Ciencia, Tecnología y Sociedad: Un Enlace hacia el Futuro

ACTUALIDAD TECNOLÓGICA

La seguridad de la información: un activo valioso de la organización

Information Security: A Valuable Asset of the Organization

José Custodio Najar Pacheco* Nubia Esperanza Suárez Suárez**

Para citar este artículo: J. Najar y N. Suárez (2015). La seguridad de la información: un activo valioso de la organización. *Revista Vínculos*, 12(1), 89-97.

Recibido: 08-enero-2015 / Modificado: 11-enero-2015 / Aprobado: 18-febrero-2015

Resumen

La seguridad de la información en las organizaciones es una problemática que aqueja a todos. Pues si bien es cierto que con la aparición constante de tecnología se facilita el darse a conocer en un mercado globalizado, así como su manejo administrativo, de igual forma se está altamente expuesta a ser atacada en cualquier momento por cibercriminales.

Metodología

Las fuentes consultadas corresponden a: revistas, bibliotecas digitales de autores tanto nacionales como internacionales, normas ISO, conocimiento de expertos como Eugene H. Spafford, de igual forma se apoyó con información de libros de prestigiosos autores; con esto se logró hacer un análisis de esta información.

Resultados

Del estudio de la información se pudo evidenciar que efectivamente el *activo más valioso* de la organización se encuentra altamente expuesto.

Conclusiones

Se puede inferir que realmente cualquier organización puede estar altamente expuesta a ser atacada por razones tanto internas como externas, en las cuales la organización no puede intervenir.

Palabras clave: Activo, ataque, información, seguridad, vulnerabilidad, delincuencia informática, fraude.

Abstract

The information security in organizations is a problem that afflicts us all, because if it is true with the constant development of technology makes himself known in a global market, is likewise highly liable to be attacked any time for cybercriminals.

Methodology

The consulted sources such as magazines, digital libraries, both national and international authors, ISO standards, expert knowledge as Eugene H. Spafford, similarly it was supported with books of prestigious authors; thus it was possible to analyze this information.

* Ingeniería de Sistemas, Universidad de Boyacá. Especialista en Telemática, Universidad de Boyacá. Especialista en Gerencia de Telecomunicaciones, Universidad Central de Bogotá. Mg(c). Seguridad Informática, Universidad Internacional de la Rioja, España. Docente en Fundación Universitaria Juan de Castellanos. jnajar@jdc.edu.co, jnajar_pw@yahoo.com.

** Ingeniería de Sistemas, UNAD. Especialista en Bases de Datos, Universidad Pedagógica y Tecnología de Colombia. Magister en Educación y TIC, Universidad Oberta de Cataluya, España. Docente en Fundación Universitaria Juan de Castellanos. nsuarez@jdc.edu.co, nubiaesya@gmail.com.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

Outcomes
The review of the information could evidence that indeed the most valuable asset of the organization is highly exposed.

Conclusions
One can infer that literally, any organization can be highly exposed to be attacked by both internal and external reasons, in which the organization can not intervene.

Keywords: Asset, cyber attacks, information, security, vulnerability, cybercrime, fraud.

1. INTRODUCCIÓN

Es importante resaltar a nivel general que la organización está constituida por la parte administrativa con el fin de lograr el objetivo, que no es ni más ni menos que lo planeado, como lo define Chiavenato [1]**;** por consiguiente, lo primordial es darse a conocer de cualquier forma y la más apropiada es la utilización de los medios de comunicación, como la red de redes, esto con el fin de posesionarse en un mercado muy competido actualmente. De igual forma, las empresas cuentan con información que debe ser únicamente del conocimiento de estas, de la parte administrativa, y es aquí donde comienza el trabajo más difícil e importante en el que pocos se interesan, y menos aún, e invierten. La falta de seguridad puede ser grave debido a diversas circunstancias, ya que estas pueden verse afectadas de gran manera; máxime cuando diariamente se sabe de ataques a los sistemas que provienen de *Organizaciones Cibercriminales***,** según el FBI [2].
La realidad es que la confianza, el desconocimiento de algunos puntos básicos en la instalación, la utilización de diversos dispositivos de última tecnología y configuración del sistema, que permiten la interacción hombre-máquina, facilitan a los delincuentes (donde participan los actores tanto internos como externos) el acceso al activo más importante de las empresas: *la Información*. Así que, por más que se cuente con capacidad y experiencia, podrán quedar vulnerabilidades que serán aprovechadas y causarán lo inesperado.
Como resultado se pretende evidenciar que realmente estamos expuestos a que la información pueda ser conocida por extraños con el fin de hacer daño tanto a instituciones como a personas; por mejor configuración e inversión que se haga en aras de la seguridad de esta, siempre se estarán al asecho de los delincuentes informáticos, por lo cual se tendrá que convivir con la inseguridad.
El objetivo del artículo es evidenciar que realmente ningún sistema es seguro cien por ciento, máxime cuando no existe concientización por parte de los administradores de las organizaciones de que se debe invertir en seguridad.

2. LA SEGURIDAD DE LA INFORMACIÓN: UN ACTIVO VALIOSO DE LA ORGANIZACIÓN

Las empresas en la actualidad, sea cual sea la razón para la cual fueron creadas, tienen como principal objetivo mantenerse en el mercado. Por lo tanto, es importante resaltar a nivel general que la organización agrupa las actividades para lograr lo que sus directivos planean [1]. De manera que para el cumplimiento de esto es muy importante darse a conocer de cualquier manera y la más apropiada es la utilización de los medios de comunicación, esto con el fin de competir y poder posesionarse en un mercado complicado, pues existe más oferta que demanda. De igual forma, la compañía cuenta con información la cual debe ser de conocimiento exclusivo de la parte administrativa, y es aquí donde comienza el trabajo más dispendioso e importante para estas, en el que pocos se interesan e invierten. La falta de seguridad puede ser grave debido a diversas circunstancias, ya que estas pueden verse afectadas de gran manera; máxime cuando se tiene conocimiento de los continuos ataques por parte de *Organizaciones Cibercriminales* [2].
Es importante advertir que las personas que hacen parte de estas organizaciones delictivas pueden operar desde cualquier parte y momento, pues es tan rentable como cualquier trabajo o negocio:

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

Todo un negocio redondo, anónimo y sin duda muy rentable, que seguramente estará dando de comer a muchas familias, eso sí, de forma fraudulenta y robando a los demás desde la comodidad de un despacho o una habitación en casa, con solo un ordenador como herramienta y amparados por la falta de regulación legislativa internacional y la ausencia de cooperación entre muchos países que facilite la investigación y la detención, estos cibercriminales llevan mucho tiempo viviendo de un negocio que sin duda promete ser muy lucrativo; como se puede ver en el Informe panda security [3].

Los sistemas de cómputo, como cualquier otro, requieren de protección, de igual forma la información; pues ya hacen parte de la red y como tal deben ser protegidos, de lo contrario equivaldría a dejar una puerta abierta a los delincuentes y esto no solo se logra al instalar un antivirus, que en otro momento muy seguramente tuvo éxito pero actualmente no, como se evidencia que más de la mitad de empresas de la región se vieron afectadas por diferentes códigos maliciosos [4].

Los antivirus por ahora, al parecer, cumplieron su labor, ya que su tarea efectivamente es la de proteger los equipos. Pero en la actualidad cualquier organización que desee protegerse no puede confiar únicamente de estas herramientas, como lo expone el autor González F. en la revista *Seguridad, Cultura de prevención TI* [5]. Por lo tanto, se debe estar preparado para no caer en manos de delincuentes que se encuentran organizados en redes de ciberdelincuentes; así mismo, se debe tener cuidado con el crecimiento en la utilización de software maligno para evitar ser atacados por la red de redes, tal como lo manifiesta la empresa Symantec, conocida por desarrollar software de seguridad y protección de la información, siendo la tercera empresa de software más grande del mundo [6].

De igual manera, para que las empresas se mantengan y continúen en un mercado competitivo deben hacer inversión en tecnología de punta, lo que permite y facilita darse a conocer en un mercado globalizado que puede ser conocido en cualquier lugar del mundo [7]; también, debe existir conciencia de que es necesario invertir para proteger la información de estas, inversión que resulta muy alta, razón por la cual posiblemente no exista disposición de hacerla ni el interés [8]; y se evidencia claramente en el artículo "El desafío de invertir en la seguridad informática y añadir valor a la empresa" [9]; ahora la preocupación es saber dónde hay más seguridad, pues existen ciertas indecisiones con respecto al lugar o modo en que puede garantizarse mayor protección; si donde se puede ver, si donde se tiene la percepción de que existe o conformarse en saber que está en algún lugar sensible donde no se puede acceder como en la nube[1]. De cualquier manera, lo primordial es saber la importancia de los datos y qué seguridad dar a cada uno de ellos, como lo expone Rosalía Sierra [10], lo cual de todos modos demanda inversión, y si las entidades optan por hacerlo actualmente, solo invierten en tecnología, dejando de lado la gestión y la capacitación que son aspectos importantes, toda vez que con esto se prepara para que cuando ocurra cualquier eventualidad de este tipo, se pueda hacer frente ante determinada situación más fácilmente [11]. Así que lo importante es contar con herramientas y procesos, pues existen Empresas que han caído en manos de los delincuentes, al tener por completo acceso al sistema así como otras que seguramente lo serán. Cada día aparece un sinnúmero de delitos

1. La nube es un equipo poderoso, no solo porque muchos de nosotros ahora se conectan a él, sino también porque muchas empresas están gastando miles de millones a granel para arriba. La unidad básica de la nueva infraestructura es el centro de datos, un edificio típicamente masivo (piensa en el tamaño de varios campos de fútbol) enormes vivienda racimos, colecciones de equipos (por lo general se cuentan por miles), conectados en red para alimentar los servicios en línea a los que hemos llegado a depender: el motor de búsqueda de Google, las operaciones de comercio electrónico de Amazon, los vídeos de YouTube, etc. El tamaño estupendo de estas granjas de servidores es una de las razones por las que incluso las más complejas búsquedas en Google arroja resultados de búsqueda en una fracción de segundo, y por qué incluso los más largos de vídeo de YouTube se inicia en cuestión de segundos etc. Recuperado de: http://spectrum.ieee.org/computing/hardware/the-cloud-is-the-computer.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

informáticos cuyo objetivo es atentar contra la información de las organizaciones como lo expone en su presentación el autor Villagrán, de la empresa Eset [12]. Conviene, sin embargo, advertir que la responsabilidad directa de la seguridad de la información está en cabeza de los directivos y empleados de las instituciones y, como tal, son conocedores de la existencia de la misma a su medida. De igual forma, la importancia que tiene esta para su normal funcionamiento, conocimiento del cual también tienen las personas ajenas a estas como los hackers, los cuales investigan de cualquier manera la forma de acceder a ellas con el fin de extraer verdades, para conseguir información y, si es el caso, pagar por esta [13]. De igual forma, vale la pena enfatizar que si bien es cierto que la tecnología facilita y permite el funcionamiento de las empresas con lo cual estas logran la prestación de un excelente servicio, responsabilidad que tienen tanto gerentes como funcionarios, cuando el sistema funciona perfectamente. Ahora bien, cuando la funcionalidad no es la más apropiada e insistentemente sufre fallas se debe preparar para garantizar la confiabilidad de la información [14]. Es preciso advertir que las situaciones mencionadas anteriormente afectan tanto al sector privado como público, en este caso a las instituciones del Estado colombiano que, ante el aumento delincuencial en el ciberespacio y la globalización que han obligado a la utilización de nuevas tecnologías, llevó a la toma de decisiones tales como: generar recomendaciones para prevenir los riesgos, realizar capacitación en seguridad y fortalecer la legislación, entre otras; esto con el fin de proteger la información [15].

Si bien es cierto el invertir en la seguridad de la información es importante, y se debe concientizar que por mejor configuración y gastos que se hagan siempre habrá amenazas de los delincuentes informáticos; así tendremos que conformarnos con saber que la información estará expuesta a ser tomada por los bandidos en cualquier momento [7]. Otras organizaciones, en aras de proteger su activo más valioso, aplican sus políticas de seguridad según la Norma ISO/IEC 27002:2013; pero también son vulneradas, como se plantea en la revista *Seguridad, Cultura de prevención TI*, así lo considera Villalobos [16], y lo contempla la norma ISO27001 Sistema de Gestión de Seguridad de la Información ISO(International Organization for Standardization); actuaciones que son válidas, máxime cuando se sabe que aparece más rápido el delincuente conociendo las vulnerabilidades que la propia tecnología [7]; sin dejar de lado que se debe asumir el riesgo por la utilización de esta, ya sea a nivel de hardware o software [17].

De otra parte, lo más sorprendente e ingenioso de los cibercriminales es el utilizar algunas aplicaciones las cuales tienen conocimiento de su popularidad, para el envío de información que al ser accesadas por desconocimiento de algunos usuarios permite apropiarse de información personal [18].

Es importante enfatizar en que para que exista de una u otra forma seguridad en las organizaciones se debe contar con técnicas, conocimientos, hardware y software ubicados de manera estratégica; todo esto con el fin de exponer menos la información [19]. Así mismo, es trascendental recalcar que con la rápida aparición de la tecnología de punta relacionada con las comunicaciones aparece de igual forma la utilización de dispositivos móviles como parte funcional de las instituciones, a través de los cuales se maneja información importante de los sistemas de cómputo de estas, la cual queda expuesta a ser conocida por los delincuentes en cualquier momento debido a probables huecos de seguridad [20]; por consiguiente, se convierte en objetivo a ser atacado.

Aunque suene un poco excéntrico, con las recientes noticias conocidas entre China y Estados Unidos, según afirmación por parte del vocero del Ministerio de la Defensa [21] y el *The New York Times* (NYT) [22], sobre posibles ataques por parte de los hackers, pues queda en tela de juicio la seguridad de la información aunque suena extraño, pues económicamente son consideradas las naciones más grandes del mundo [23]. Por tal razón, se evidencia que la información que circule por la red está altamente expuesta a ser identificada. Con lo cual se puede dar por válida la afirmación que hasta hace

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

poco se podía suponer una simple hipótesis: efectivamente, ningún sistema es completamente seguro por muchas y diversas razones, como lo sintetiza la afirmación: "Toda Organización es vulnerable y no existe un 100% de prevención", según confirma y expone Franklin Noguera [24]. Al parecer tiene cierta validez cada vez que no existe una verdadera convicción de seguridad o definición de la misma, pues es una ficción pensar que existe verdaderamente la seguridad de la información, y por consiguiente un sistema seguro en su totalidad [25], citado por Gómez, D. y Quintero, M. [26].

En la actualidad, las personas e instituciones hacen uso de la red de redes para el desarrollo de sus actividades, y el acceso para el caso de los funcionarios, se hace desde cualquier lugar. No obstante, se deben guardar las mínimas normas de seguridad: en esta ocasión la configuración del *firewall*[2] del sistema Operativo y el limitado acceso a las aplicaciones de los funcionarios que debe darse de acuerdo con el desarrollo de las actividades [27]. De igual manera, el constante crecimiento de las empresas en los últimos tiempos y el desarrollo tecnológico relacionado con la movilidad han llevado a que exista un mayor uso de los diferentes dispositivos, que al día de hoy son diversos y de fácil manejo, para ser utilizados tanto para venta de sus productos y servicios como para el desarrollo de las labores de funcionarios. Lo que ha llevado a que se deba hacer inversión, pues el objetivo último es la protección de la información que cursa por la red; por lo cual se debe señalar que entre más tecnología se utilice, mayores serán los costos que se deben hacer en seguridad, pues más puntos se deben asegurar [28].

Así mismo, es importante resaltar que la delincuencia aprovecha las oportunidades, siempre están atentos ya sea para apropiarse de tarjetas de crédito o cuentas de correo electrónico. No obstante, la forma de conocer el ilícito por parte de los afectados es diferente, ya que una vez se conoce el robo de las tarjetas, estas se pueden bloquear de manera rápida y posiblemente se evite que el delincuente se salga con las suyas. En el caso de las cuentas de correo, una vez irrumpida, se dificulta un poco más su conocimiento. Así se tendrá que aceptar la convivencia con los delincuentes, aunque no estemos de acuerdo, y si hasta el momento no cuentan con información que pueda hacer daño estarán atentos a seleccionar aquella que les pueda servir tal como datos personales y claves de cuentas bancarias, con lo cual causan pérdidas millonarias [6].

Podemos darnos cuenta de que efectivamente los ladrones tienen en mente lograr un objetivo en común, apropiarse de información ya sea para utilizarla en su propio beneficio o para venderla y hacerle daño a las organizaciones. De cualquier modo, su meta es obtener ganancias; pero vale la pena destacar que esto lo logran los maleantes, de una u otra forma, porque los usuarios así lo permiten al caer en las trampas y engaños tendidos por los facinerosos informáticos o hackers. Pero hay que resaltar que estos van siempre por información de tipo financiero o comercial, pues es en últimas la que les interesa [29].

Así como existen bandidos humanos que delinquen en la calles sembrando el terror, de igual forma se encuentran atacantes que atentan en la red para apropiarse de información y usarla a su antojo, y hasta utilizarla para cometer crímenes informáticos. Todo esto redunda constantemente en obtener prebendas de tipo económico, pero siempre existirá responsabilidad de los beneficiarios al declinar fácilmente en la farsa tendida por los delincuentes [30].

En este sentido, los encargados de la manipulación de los equipos tienen el compromiso directo ya que no poseen o no aplican las políticas de seguridad relacionadas con la continua actualización de antivirus y que al no impedir la instalación de programas

2. Un firewall es software o hardware que comprueba la información procedente de internet o de una red y, a continuación, bloquea o permite el paso de esta al equipo, en función de la configuración. Un firewall puede ayudar a impedir que hackers o software malintencionado (como gusanos) obtengan acceso al equipo a través de una red o de internet. También puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos. Recuperado de: http://windows.microsoft.com/es-co/windows/what-is-firewall#1TC=windows-7.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

que al ser ejecutados causan desastres, entre otras**;** software que seguramente fue instalado con o sin conocimiento o programas espía, etc. Así, en estas condiciones, los usuarios utilizan los servicios en línea, lo cual será desconcertante y nada halagador para ellos y muy beneficioso para los delincuentes. Esto se puede mejorar con la utilización de sistemas para evitar fraudes, los cuales no son utilizados por la mayoría de usuarios [31].

El constante desarrollo tecnológico ha facilitado que en la actualidad exista un alto porcentaje de usuarios que utilizan la red para manejar lo relacionado con las transacciones nacionales o internacionales. Igual sucede en nuestro país, donde encontramos un porcentaje menor pero representativo que no utiliza este sistema, pues lo considera inseguro, máxime cuando se puede hacer desde cualquier dispositivo móvil y lugar. Cierto es que debe existir responsabilidad de todas las partes que hacen funcional el sistema y como tal también son responsables de la seguridad de una u otra manera [32], sin negar es que es difícil poner todas las partes de acuerdo por múltiples y diversas razones. Así que en cualquier momento se estará expuesto una vez más a que exista ofensiva por los delincuentes; sobre todo cuando cada vez se utilizan más sofisticadas formas de acometer. Tan así que es difícil e imposible su detección y por consiguiente su protección [33]**.** Lo mismo sucede con las organizaciones del sector salud que utilizan la tecnología y las comunicaciones para la atención de pacientes, realización de pruebas médicas o para evaluar exámenes diagnósticos. Vale la pena destacar la importancia que se le debe dar a la seguridad de la información y a la utilización de las nuevas tecnologías actualmente y en un futuro, lo que sin lugar a duda es un reto [34]. De igual manera, existe la preocupación por el uso de dispositivos y aplicaciones móviles que, si bien es cierto que facilitan la tarea de quienes adelantan esa loable labor en este sector, representan un riesgo en lo relacionado con la protección de datos que tienen que ver con las historias clínicas; ya que primero se piensa en la funcionalidad más que en la seguridad [35].

Ante lo anterior, es importante enfatizar que las empresas desarrolladoras de software deben cumplir y ser responsables en lo referente a la seguridad de las aplicaciones, de este modo se tendrá éxito si se cumple. Sin dejar de lado que, efectivamente, en este punto es importante e imprescindible contar con la aplicación de la familia de normas ISO 27000[3]; en este caso la ISO 27799[4] y la ISO/IEC TR 27015[5], relacionadas con la seguridad informática y que están obligadas a cumplir actualmente, tanto en el sector sanitario como financiero y de seguros [36].

Bajo este cúmulo de situaciones, y otras que se desconocen, valdría la pena cuestionar ¿qué tan segura o que tanto se conoce la seguridad de la información como el activo más valioso de la organización?, la cual, seguramente causa incertidumbre pues no existe la repuesta más apropiada. Por consiguiente, en efecto se duda de la seguridad de la información en las instituciones. Lo expuesto permite plantear algunos interrogantes, entre estos: ¿por qué al efectuar una correcta instalación y configuración *del sistema* lo podemos hacer menos vulnerable?, o, ¿por qué al continuar renovándolo e instalando actualizaciones es posible disminuir la fragilidad?, o ¿si se hace más inversión en seguridad, se estará menos expuesto? Como gran punto final, por estas y por otras tantas razones que se desconocen, comparto y estoy de acuerdo con la afirmación referente a la seguridad expresada por el experto en seguridad informática Eugene H. Spafford [37]:

3. ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información.
4. ISO 27799: Publicada el 12 de Junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.
5. ISO/IEC TR 27015: Publicada el 23 de Noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

3. CONCLUSIONES

La información como el activo más importante de una organización requiere especial atención en su cuidado y/o protección. Es la que da las pautas para encauzarla por la senda del éxito. Así que la configuración e instalación inicial de los *sistemas* de cualquier empresa es fundamental para su correcto funcionamiento, ya que constituye el punto de partida para evitar que se dejen vulnerabilidades, que al ser descubiertas por intrusos, afectarían la correcta funcionalidad de los sistemas. Todo lo que se haga por la seguridad de la información en las instituciones, no importa su tamaño, será muy importante. No obstante, esto no garantiza que las amenazas no estén presentes, pues se tendrá que convivir con ellas a pesar de los arduos esfuerzos de los directivos y empleados.

Al ser la información el activo más valioso, éste requiere de una particular protección así como de inversión; pero por más que se invierta, siempre se estará expuesta ya que la consecución de la seguridad depende tanto de factores internos como externos, por lo que se necesita de una perfecta sincronización y es precisamente lo que no se logra. Sobre todo cuando existen y/o se han dejado vulnerabilidades en los sistemas que son aprovechadas por los delincuentes, lo cual permite que se organicen y creen organizaciones cibercriminales. Por tal razón se convierte en un negocio que deja muy altos dividendos y cuya actuación se da a nivel tanto nacional como internacional, afectando a todos los sectores e instituciones públicas y privadas.

Así que siempre se estará amenazado; por más que se luche por mantener la seguridad de la información en cualquier organización, constantemente se estará expuesto a eventuales sorpresas. Pues, por mejor configuración e inversión que se haga, continuamente se estarán acechando los delincuentes. Así, tendremos que conformarnos con reconocer que la información estará expuesta a ser utilizada por estos, si así lo quieren en cualquier momento.

4. REFERENCIAS

[1] I. Chiavenato*, Introducción a la Teoría General de la Administración*, México.: Mc Graw Hill., p. 154, 2006,

[2] T. Patrick, "Segu. Info NewS Noticias sobre Seguridad de la Información", 30 Marzo. 2010. [En línea]. Disponible en: http://blog.segu-info.com.ar/2010/03/fbi-enumera-los-10-principales-puestos.html#axzz30wysVI3I.

[3] Panda Security, "PRENSA PANDA SECURITY", 20 Enero 2011. [En línea]. Disponible en: http://www.pandasecurity.com/spain/mediacenter/src/uploads/2014/07/Mercado-Negro-del-Cybercrimen.pdf.

[4] Centro de Prensa de ESE, "Centro de Prensa de ESE", 30 Abril 2013. [En línea]. Disponible en: http://www.eset-la.com/centro-prensa/articulo/2013/latinoamerica-50-de-empresas-sufrio-ataques-malware-durante-2012/3109.

[5] F. C. González., "El futuro no pertenece a los antivirus", *Seguridad, Cultura de prevención TI,* No. 13, p. 26, 2012.

[6] M. Romero, "Portafolio .co", 18 Junio 2010. [En línea]. Disponible en: http://www.portafolio.co/detalle_archivo/MAM-4014370.

[7] J. J. Cano M., *Computacion forense descubriendo los rastros informaticos*, Primera. ed., México.: Alfa omega Grupo Editor, S.A. de C.V., 2009.

[8] L. Diez Grajales, "Innovan en el cuidado de datos", 9 Junio 2010. [En línea]. Disponible en: http://www.eluniversal.com.mx/finanzas/79909.html.

[9] L. Custodio, "El desafío de invertir en la seguridad informática y añadir valor a la empresa", *El País*, 29 Julio 2013. [En línea]. Disponible en: http://www.elpais.com.uy/economia-y-mercado/desafio-invertir-seguridad-informatica-anadir.html.

[10] R. Sierra, "La nube es, cuando menos, más fiable que los carritos de HC", *Club Gertech*, 3 Mayo 2012. [En línea]. Disponible en: http://clubgertech.blogspot.com.es/2012/05/la-nube-es-cuando-menos-mas-fiable-que.html.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

[11] F. Catoira, "Prevenga el código malicioso en su empresa", *EF El Financiero*, 19 Mayo 2013. [En línea]. Disponible en: http://www.elfinancierocr.com/tecnologia/codigo_malicioso-malware-ataques-ciberdelincuentes_0_301169905.html.

[12] El País, "Campaña sobre la seguridad en Internet", *El País*, 16 mayo 2013. [En línea]. Disponible en: http://www.elpais.com.uy/economia/noticias/campana-sobre-la-seguridad-en-internet.html.

[13] C. S. ALFONZO A., *Contextotmt.net*, 10 Septiembre 2011. [En línea]. Disponible en: http://www.contextotmt.net/base/unilever/index2.php?option=com_content&do_pdf=1&id=27807.

[14] J. C. Daccach T., "¿Cómo está su plomer+ía digital?", *Delta*, 24 Febrero 2014. [En línea]. Disponible en: http://www.deltaasesores.com/articulos/tecnologia/7206-icomo-esta-su-plomeria-digital.

[15] J. M. Cárdenas, "Política de ciberseguridad y ciberdefensa", *Portafolio.co*, 28 Agsoto 2011. [En línea]. Disponible en: http://www.portafolio.co/columnistas/politica-ciberseguridad-y-ciberdefensa.

[16] J. Murillo Villalobos, "Gestión de incidentes de seguridad informática con agentes inteligentes", *Seguridad Cultura de prevención TI,* No. 14, p. 30, Julio-Agosto, 2012.

[17] A. Castro Ramírez, "Riesgo tecnológico y su impacto para las organizaciones-Parte I", *Seguridad, Cultura de prevención TI,* No 14, p. 30, Julio-Agosto, 2012.

[18] C. RUIZ VEGA, *EF El Financiero*, 20 Enero 2014. [En línea]. Disponible en: http://www.elfinancierocr.com/tecnologia/Hackers-supuesto-WhatsApp-distribuir-informatica_0_449955019.html.

[19] A. Aguilar Dominguez, "Firewall de bases de datos", *Seguridad, Cultura de prevención TI,* No. 18, p. 34, Mayo-Junio, 2013.

[20] M. J. Romero Cortes, "Dispositivos móviles, en la mira de los 'hackers'", *Portafolio.co*, 20 mayo 2011. [En línea]. Disponible en: http://m.portafolio.co/negocios/dispositivos-moviles-la-mira-los-%E2%80%98hackers%E2%80%99/?tamano=grande.

[21] CNN Expansión, "China reporta ciberataques desde EU", *CNNExpansión*, 28 febrero 2013. [En línea]. Disponible en: http://www.cnnexpansion.com/tecnologia/2013/02/28/china-reporta-ciber-ataques-desde-eu.

[22] Elmostrador.mundo, "Hackers chinos atacan The New York Times tras artículo sobre riqueza de primer ministro Wen Jiabao", *Elmostrador.mundo*, 31 enero 2013. [En línea]. Disponible en: http://www.elmostrador.cl/mundo/2013/01/31/hackers-chinos-atacan-the-new-york-times-tras-articulo-sobre-riqueza-de-primer-ministro-wen-jiabao/.

[23] Emol.economia, "Presidente chino señala que EE.UU. y su país tienen 'muchísimos intereses en común'", *Emol.economia*, 19 marzo 2013. [En línea]. Disponible en: http://www.emol.com/noticias/economia/2013/03/19/589143/presidente-chino-senala-que-eeuu-y-su-pais-tienen-muchisimos-intereses-en-comun.html.

[24] D. L. Salas, "EF El Financiero" Enero 29 2013. [En línea]. Disponible en: http://www.elfinancierocr.com/tecnologia/inseguridad_cibernetica-Deloitte-malware_0_236376366.html.

[25] M. M. P. L. Marianella Villegas, "Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática", *Redalyc.org,* Vol. 10, No 1, p. 5, 2011.

[26] D. M. Gómez Vargas y M. Quintero Polania, "Seguridad informática", *Scribd*, 2008. 13 junio 2014 [En línea]. Disponible en: http://www.scribd.com/doc/6317119/Seguridad-a-Doc-Word1.

[27] M. F. Landaeta, "Mejore la seguridad en Internet con estos 10 tips", *EF EL FINANCIERO.*, 13 junio 2014. [En línea]. Disponible en: http://www.elfinancierocr.com/pymes/Mejore-seguridad-Internet-tips_0_207579906.html.

[28] F. Quinonez, "Ricardo Santos: gerente regional de Dell para CA", *SIGLO21.com.gt*, 27 mayo 2010. [En línea]. Disponible en: http://www.s21.com.gt/pulso/2010/05/27/ricardo-santos-gerente-regional-de-dell-para-ca.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.

[29] Portafolio.co, "A reforzar seguridad informática", *Portafolio.co*, 27 febrero 2009. [En línea]. Disponible en: http://www.portafolio.co/detalle_archivo/MAM-3079524.

[30] Portafolio.co, "La importancia de la seguridad en Internet", *Portafolio.co*, 30 marzo 2011. [En línea]. Disponible en: http://m.portafolio.co/detalle_archivo/MAM-4474080.

[31] Portafolio.co, "Usuarios no conocen toda la seguridad en banca 'online'", *Portafolio.co*, 19 septiembre 2011. [En línea]. Disponible en: http://m.portafolio.co/economia/usuarios-no-conocen-toda-la-seguridad-banca-%E2%80%98online%E2%80%99?tamano=grande.

[32] B. Rozo, "Portafolio.co" 7 Noviembre 2012. [En línea]. Disponible en: http://www.portafolio.co/detalle_archivo/DR-70329.

[33] R. Lozano, "Easy Solutions, con socio de Estados Unidos", *Portafolio.co*, 29 mayo 2013. [En línea]. Disponible en: http://www.portafolio.co/negocios/inversion-easy-solutions.

[34] M. Frowein, "Gestión en Salud Pública", 26 febrero 2013. [En línea]. Disponible en: http://saludequitativa.blogspot.com/2013/02/retos-de-las-tic-en-lo-sanitario.html.

[35] R. Sierra, "Es momento de preocuparse por la seguridad de las 'app'", *Diario Médico*, 24 febrero 2014. [En línea]. Disponible en: http://comunicacion.fenin.es/prensa/n38716_dm3.pdf.

[36] D. Davila, "Aun con crisis, tecnológicas suman empleos", *La Voz*, 28 febrero 2014. [En línea]. Disponible en: http://www.lavoz.com.ar/negocios/aun-con-crisis-tecnologicas-suman-empleos.

[37] M. Santos, "Seguridad Informática febrero-junio 2014.," 09 Abril 2014. [En línea]. Disponible en: http://seginf2014.blogspot.com/2014/04/informatica-y-mascotas-no-mezclar.html.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 12, No 1 (enero-junio 2015). pp. 89-97. Universidad Distrital Francisco Jose de Caldas-Facultad Tecnologica.