Visión Electrónica Vol. 11 No. 1 (2017) • Enero-Junio • p.p. xx-xx • ISSN 1909-9746 • ISSN-E 2248-4728 • Bogotá (Colombia)

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Visión Electrónica

Más que un estado sólido

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

https://doi.org/10.14483/22484728.12345

VISIÓN ELECTRÓNICA

VISIÓN DE CONTEXTO

Exposición del activo más valioso de la organización, la "información"

Exposure of the most valuable asset of the organization, the "Information"

José Custodio Najar Pacheco[1]

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Enviado: 15/08/2016
Recibido: 22/09/2016
Aceptado: 13/11/2016

Palabras clave:
Activo
Ataque
Cibercriminales
Seguridad informática
Vulnerabilidad.

RESUMEN

A fin de mantenerse activas las organizaciones deben contar con tecnología de punta que facilite su identificación en un mundo globalizado; la forma más fácil, sencilla y económica es haciendo uso de la red de redes. Es aquí donde comienza el trabajo más complicado y al que los administrativos poco valor le dan y mucho menos invierten: dotar de seguridad el activo más valioso de cualquier Institución: *la Información*. El presente artículo reflexiona sobre los riesgos a los que se expone la información si no se surten las mínimas normas de seguridad: manejo, manipulación, cuidado y asistencia, entre otras. Se resalta que las organizaciones y usuarios tienen la oportunidad de desarrollar de forma fácil actividades desde cualquier lugar, siempre que se tenga en cuenta la cultura de la capacitación y se cuente con planes de respuesta a incidentes, de manera que ellas puedan seguir prestando sus servicios, inclusive si no se tiene el control de la funcionalidad de internet.

Keywords:
Asset
Cyberattack
Cybercriminals
Information security
Vulnerability.

ABSTRACT

Organizations to stay active must have technology, which facilitates their identification in a globalized world; the easiest, simple and economical way is using the World Wide Web; this is where the hardest work begins and managers give little value; and even less invest on the security of the most valuable asset of any institution: ïnformation". This article reflects about the risks to which the information is exposed if the minimum safety standards are not met: management, handling, care and assistance, among others. It is highlighted that organizations and users have the opportunity to easily develop activities from anywhere, as long as the culture of training is taken into account and incident response plans are in place; So that Organizations can continue to provide their services even if they do not have control of Internet functionality.

[1]Ingeniero de Sistemas; especialista en Telemática, Universidad de Boyacá, especialista en Gerencia de Telecomunicaciones, Universidad Central; magister Seguridad Informática, Universidad Internacional de la Rioja; docente Fundación Universitaria Juan de Castellanos. Correo electrónico: jnajar@jdc.edu.co

Citar este artículo como: J. C. Najar "Exposición del activo más valioso de la organización, la "información"" . Visión Electrónica, algo más que un estado sólido, Vol. 11, No. 1, xx-xx, enero-junio 2017.

1. Introducción

Es importante resaltar, a nivel general, que en la estructura de una organización, la parte administrativa es la que tiene como fin lograr el objetivo de lo que se planea. Últimamente, en este contexto ha surgido la importante tarea de darse a conocer de múltiples maneras y la más apropiada y económica es utilizando la Internet como medio masivo de comunicación. Esto, como parte de la estrategia de mercado que beneficia tanto a demandantes como oferentes. Así mismo, como es obvio, existe información que solo es de conocimiento de la administración y como tal debe ser protegida, para lo cual debe contarse con la tecnología adecuada y el personal capacitado. Lo anterior se logra con una inversión suficiente que minimice riesgos, ya que la información al circular por la red de redes está altamente expuesta ante la ampliación de la existencia de vulnerabilidades que pueden ser aprovechadas por *Organizaciones Cibercriminales* [1].

De otra parte, se pretende dar a conocer que sin duda se está inmensamente expuesto a que la información pueda ser conocida por personas no autorizadas tanto internas como externas a la organización; por preferible configuración e inversión que se haga en aras de la seguridad de la Información siempre estarán al acecho los delincuentes informáticos, razón por la cual se tendrá que convivir racionalmente con la inseguridad.

De igual forma, sería desorbitadamente imposible pensar al menos por un segundo cómo sería la sociedad actual al no contar con tecnología, pues cada día dependen más de ella las organizaciones, la banca, los grandes avances tecnológicos, el desarrollo de proyectos, la salud, los gobiernos, la educación y un sin número de actividades se desarrollan gracias a la funcionalidad y a su utilización. Se toman decisiones transcendentales sobre la base de resultados y procesos.

Como se evidencia se maneja información muy importante y trascendental para el cumplimiento de la misión de las organizaciones, que debe ser responsabilidad y confidencialidad de cada uno de los que hacen parte de estas, pero desafortunadamente no es así, pues en algunas oportunidades no se cuenta con el mínimo de compromiso de la parte tecnológica, menos de los administrativos; así, por diversas razones una vez más se tendrá que aceptar que de una u otra forma se está buscando la solución a un problema, del cual también se hace parte.

2. Exposición del activo más valioso de la organización, la “información”

Cualquier organización productiva, sea cual sea la misión para la cual fue creada, tiene como objetivo primordial mantenerse vigente en el mercado. Por consiguiente, es necesario resaltar, a nivel general, que esta prioriza y agrupa actividades para lograr lo que sus directivos planean [2].

Así que, para cumplir lo proyectado, se asume la importancia de darse a conocer; y la vía más económica y masiva para hacerlo es la Internet. En la actualidad las personas utilizan este medio para consultar cualquier producto o información que necesiten, los datos son concluyentes: el 80 % consultan antes de comprar, según estudio de la empresa de tecnología ComScore para América Latina [3].

No obstante, la inseguridad en Internet ha venido aumentando, tanto que algunas compañías han decidido preocuparse por este tema que, además de complicado, afecta todos sus ámbitos. Es así que existen Centros de Seguridad online para ayudar a los usuarios de Internet a desarrollar destrezas de seguridad [4]. de igual forma, es claro entender que la información de cualquier organización tiene riesgos al transitar por la red de redes; esta se puede ver afectada por diferentes razones y en muchas oportunidades no depende de las capacidades técnicas utilizadas por las empresas por más experiencia que se tenga, sino de su forma de detectarlas pues entran a formar parte de los espacios IP en los cuales si ademas de ser usuarios es difícil intervenir, lo es menos controlar. De lo anterior, existe la preocupación por la seguridad informática que incluye: garantizar la información, asegurar las comunicaciones y la protección de los activos; incorporándose los hallazgos a los planes de seguridad de las entidades. Sin embargo, queda la preocupación de exponerse a múltiples dificultades por los diferentes riesgos tecnológicos externos, tanto lógicos como de reputación [5].

De igual manera, cabe señalar que de una u otra forma existe responsabilidad por parte de los usuarios al no contar con las mínimas normas de seguridad (por ejemplo, se ponen claves a los equipos y dispositivos de comunicación que entran a formar parte de Internet sencillas de identificar), lo cual facilita a los delincuentes hacer lo que se les antoje. Un ejemplo evidente está documentado: en un solo día se identificaron un gran número de equipos como routers, impresoras y otros accesorios, que respondieron a diversas órdenes, luego de efectuar escaneos a las IP [6].

Ante tales situaciones y debido al incremento de la inseguridad, así como al constante hurto de información a las personas, organizaciones y agencias, entre otras, tanto a nivel nacional como internacional se ha multiplicado el número de instituciones dedicadas a la seguridad; y se evidencia en que han venido aumentando sus inversiones y, por consiguiente, sus ganancias [7].

De la misma manera sucede con el constante aumento en la utilización de Internet para la prestación de diversos servicios en diferentes sectores de la sociedad. Esto ha dado lugar a la presencia de empresas que prestan el servicio de seguridad informática [8]; lo cual demuestra que efectivamente la seguridad es responsabilidad de todos. De este modo, al parecer, se da una proporcionalidad directa: se está aprovechando la oportunidad de mercado en evidencia de que efectivamente existe inseguridad. Así, para no alejarse tanto de la realidad, en los últimos años en Colombia se han preocupado por llegar con tecnología para dar servicio de Internet a gran cantidad de población y en los lugares más alejados del pais, como política de los gobiernos, lo cual parece plausible; pero no se ha preocupado, ni posiblemente se han cuestionado acerca de los riesgos que ello implica. Se han encontrado resultados altamente preocupantes: pérdidas que alcanzan el orden de los 95 millones de dólares para el año 2013, evidenciándose que Colombia se encuentra entre los países más atractivos para ser atacados por los *ciberdelincuentes* [9]. Lo anterior se presenta porque no existe concientización sobre la importancia de la seguridad de la información y la consecuente ausencia de inversión de recursos en el tema.

De otra parte, es importante recalcar que la delincuencia no mide su accionar: actúa de tal manera que no le interesa a quien afecte. El caso de los menores de edad es alarmante: al hacer uso indiscriminado de Internet a través de diversos dispositivos de comunicación se convierten en presa fácil de los delincuentes; por consiguiente, se exponen altamente a riesgos contra su integridad. En consecuencia, se tiene que entrar a contrarrestar este accionar con inversión para adquisición y utilización de herramientas preventivas [10].

En el anterior sentido, hoy en día la delincuencia ha tocado fondo: ha llegado a secuestrar los equipos de cómputo para pedir rescate por ellos. Estas bandas criminales se encuentran organizadas para delinquir utilizando estrategias para acceder remotamente, por lo que el usuario se ve en la necesidad de pagar para utilizarlos, de lo contrario corre el riesgo de perder su información; y aún, a veces, accediendo a tales peticiones de igual forma la pierden pues deben reiniciar su equipo y pagar por ello. Para solicitar el rescate utilizan las direcciones de Internet de sus víctimas con notas intimidatorias [11].

De lo expuesto, se puede indicar que, con la aparición del Internet, la humanidad ha podido evolucionar de manera vertiginosa en aspectos como el conocimiento, la virtualización, el hacer real lo irreal, tener la posibilidad de cumplir sueños y hasta salvar vidas. Además de un sinnúmero de posibilidades y servicios que han permitido el desarrollo de ciertas sociedades a todos los niveles. No obstante, su crecimiento ha continuado cada día con el fin de prestar más y mejores servicios. La aparición de por ejemplo Facebook y Twitter ha sido importante pues ha facilitado y permitido el bienestar para la comunidad de usuarios; pero desafortunadamente en múltiples oportunidades no han sido utilizadas de forma apropiada, pues son empleadas para delinquir debido a su popularidad aprovechando la poca experticia del usuario por desconocimiento o confianza, permitiendo caer fácilmente en trampas montadas por los ciberdelincuentes: contagio de los equipos, robo de información vital; asuntos que en manos equivocadas puede causar daños irreversibles [12]. De igual forma sucede con la utilización de estas redes, tanto a nivel personal como empresarial, pues al usar dispositivos móviles para adelantar actividades propias de la organización, dispositivos altamente vulnerables que tienden a ser extraviados, y donde más de la mitad de usuarios no pone contraseñas o passwords dejan en entredicho las responsabilidades y la seguridad de la información de las instituciones [13].

Pese a todo lo anterior, cabe señalar que las organizaciones con el propósito de prestar un mejor servicio, siguen la tendencia de utilizar tecnología de punta; así mismo, frente a la variedad de los servicios que ofrecen, lo excelente y respetable, desde diferentes puntos de vista, no asumen de manera responsable los riesgos que provienen de la utilización de los mismos, como: computación móvil, el uso de servicios en la nube y la administración en el uso de las redes sociales. Así, la información está cada vez más expuesta al riesgo, como se puede evidenciar en la encuesta documentada en [14]: el 72 % acepta que hubo aumento del riesgo informático, el 56 % admite que la estrategia en seguridad debería modificarse y el 46 % identificó peligros al interior de las mismas empresas.

Conviene, sin embargo, advertir que de cualquier manera existe responsabilidad en la inseguridad por parte de los encargados de la protección de los datos, pues son los que cometen en ocasiones anomalías graves

con respecto a la seguridad. Así mismo, sucede con el Departamento de Tecnologías de la Información en las organizaciones (DTI), que incurre en fallas en las que se ve comprometida la información de la institución, por lo que se hace necesario invertir en su capacitación [15].

Por lo anteriormente expuesto, resulta irónico que mientras existe una constante preocupación en nuestro medio por velar por el cuidado de la información, en algunas organizaciones se cuenta con un alto porcentaje de vacíos de protección relacionados con la seguridad Informática, así como otras que no muestran el interés por la protección de los datos, según lo revela la encuesta dada en [16]. Si bien es cierto el Internet permite ser utilizado de manera muy sencilla y sin mayor complicación, debe existir responsabilidad al momento de adquirir productos o hacer transacciones. Los ladrones informáticos están al acecho monitoreando el tráfico constantemente, con el fin de buscar la oportunidad de *hackear* y apropiar datos personales. Por lo tanto, algunas empresas, para evitar este tipo de situaciones y minimizar el riesgo, dan a conocer algunas recomendaciones importantes que vale la pena tener en cuenta: comprar en sitios reconocidos; sistemas y aplicaciones actualizadas; evitar enlaces en correos electrónicos sospechosos; no utilizar conexiones Wi-Fi de dudosa confiabilidad, entre otras, [17].

De este modo personal o corporativamente, es importante estar dispuesto a seguir funcionando en caso de presentarse alguna adversidad de la cual ninguno está exento. Las empresas deben prepararse y contar con un plan de respuesta a incidentes para poder restablecerse y continuar funcionando. Lamentablemente, a nivel de Latinoamérica, solo el 26 % de las organizaciones cuenta con estos planes; según encuesta realizada por ESET Security Report Latinoamérica [18]. En este mismo sentido, y como consecuencia valores significativos de pérdidas representados en dinero y tiempo, otros estudios así lo demuestran, como por ejemplo el realizado por el Ponemon Institute y auspiciado por HP®, denominado: *Costo del crimen cibernético en 2012* [19].

En síntesis, es inevitable el uso de Internet y los servicios que ofrece, a pesar del riesgo que representa, pues de una u otra manera existe dependencia de ellos por la necesidad organizacional y personal del acceso a cuentas web. Es decir, si son identificadas anomalías de seguridad graves inconvenientes se generan en los usuarios.

Por lo anterior, para evitar ser presa fácil por parte de los *hackers* es recomendable:

- La creación de correos diferentes de acuerdo con los servicios que se requieran utilizar.
- La instalación de herramientas de seguridad en los navegadores [20].
- Restringir los dispositivos móviles celulares para uso y almacenamiento de información sensible.

Ante la idea de que los ciberdelincuentes cada día tienen nuevos retos, pues no solo se satisfacen con el robo de la información sino que quieren tomar el control de las organizaciones [21], vale la pena señalar que anteponer controles a la visibilidad segura de las mismas puede realizarse desde cualquier latitud durante la instalación y configuración del protocolo de comunicaciones TCP/IP, protocolo que, a propósito, desde su inicio no fue diseñado para ser utilizado en redes públicas por lo cual no hubo preocupación por su seguridad, asunto que ya es asumido como necesidad de seguridad de las tecnologías de la información. Por lo anterior, en la construcción de la confianza para una sociedad [22], ratificado por la Computación Forense[2], debe existir seguridad tanto a nivel de la organización como fuera de ella [23]. Los ataques pueden venir de donde menos se piensa [24]. De esta manera, al ser el primer contacto con el mundo exterior de una organización, la configuración y utilización de TCP/IP debe atender la confiabilidad y vulnerabilidad relacionadas en los diferentes Boletines de Seguridad de Microsoft, y Linux [25–29].

De otra parte, con respecto al protocolo RDP (Remote Desktop Protocol (RDP, por sus siglas en inglés) que también es frágil, [30], es importante resaltar que para mantenerse en un mercado competitivo debe contarse con tecnología para el desarrollo y control de actividades diarias de dirección y salvaguardar la información. Pero en la mayoría de los casos se desconoce qué tan seguros están los activos, porque las organizaciones no invierten y menos asignan un rubro o porcentaje de su presupuesto para la seguridad informática.

Así, la seguridad de la información en las organizaciones, se ha convierte en un obstáculo difícil de solucionar al no contar con el apoyo por parte los directivos, pues no son conscientes de que se debe brindar el soporte necesario de manera incondicional, en aras de minimizar la protección de la información.

[2]Computación forense (computer forensics): Disciplina de las ciencias forenses, que procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; los elementos propios de las tecnologías de los equipos de computación ofrece los elementos propios de las tecnologías de los equipos de computación así como un análisis de la información residente en dichos equipos.

De la V Encuesta Latinoamericana de Seguridad de la Información Informe 2013 [31] y VIII Encuesta Latinoamericana de Seguridad de la Información, Nuevos horizontes para América Latina. Junio 2016 [32], se destaca que efectivamente con respecto a la información relacionada, con los "obstáculos de implementación de la seguridad de la Información", en el ítem Falta de apoyo directivo: para el año 2009 este fue del 18.50 % comparado con el del año 2016 que corresponde al 32.3 % aumento en 13,80 puntos porcentuales, de modo que se puede concluir que en verdad no existe un verdadero compromiso de las directivas frente a la organización, arriesgando de esta manear la seguridad la información (Tabla 1).

Tabla 1: V Encuesta Latinoamericana de Seguridad de la Información Informe 2013 Y Viii VIII Encuesta Latinoamericana de Seguridad de la Información, Nuevos Horizontes para América Latina [31]

Año	2009	2010	2011	2012	2013	2015	2016
Falta de apoyo directivo	18.50 %	15.21 %	16.37 %	35.27 %	48.33 %	41.6 %	32.3 %

De este modo se puede concluir que es necesario que se realice la correcta configuración y utilización de los protocolos de comunicaciones: TCP/IP no confiable totalmente [26], y el RDP (Remote Desktop Protocol) [27]; además de invertir en personal capacitado y con experiencia, que se logra si lo permite la dirección de la organización. Por consiguiente, es fundamental recalcar y enfatizar en la importancia que se debe dar a la correcta instalación y configuración del sistema ante el pleno conocimiento de la existencia de "Vulnerabilidades" que, de no ser identificadas a tiempo, conllevan a dejar una puerta abierta al público, sin vigilancia. Se reitera igualmente que identificar a tiempo las diferentes vulnerabilidades ante el constante aumento de delitos cibernéticos perpetrados por organizaciones criminales permite tomar algunas decisiones de colaboración con otras Instituciones con el fin de ayudar a identificar iniciativas relacionadas con la seguridad [30].

Por otro lado, para el 2013 se presentaron variantes delictivas: hurto de equipos o extravío de información publicada accidentalmente, extorsión, robo de información por parte de los hackers relacionada con tarjetas de crédito, números de teléfono, fechas de nacimiento y número de documentos; además de información financiera.

El aumento de estos ilícitos, en lo que se refiere a los ataques más específicamente con *ransomware*[3] en la región, se han venido cometiendo de forma más sofisticada y por consiguiente incrementándose hasta en un 500 % con respecto al año 2012 y en un 750 % en el 2016 [33], situación que realmente resulta incómoda y preocupante; pero la exposición disminuye si se hace inversión a la medida y de acuerdo con planes plenamente establecidos. En el caso regional: Argentina, Brasil, Chile y Colombia, ocupan los primeros lugares en amenazas cibernéticas financieras en América Latina [34].

Por otra parte, con la aparición de nuevos dispositivos tecnológicos, se hace necesaria su adaptación para poder ser utilizados. Desde esta perspectiva, se tienen que diseñar nuevas aplicaciones para su funcionalidad segura. En caso de usarse con Internet (o el Internet de las cosas), los riesgos son inminentes y si hasta ahora no ha pasado nada es porque nadie lo ha vulnerado; no porque realmente exista una verdadera protección. Luego, entendiendo que la seguridad total en la red de redes es imposible de lograr [35], a pesar de que la utilización de estos dispositivos se extienda a todos los campos del quehacer diario, pues efectivamente facilitan las tareas,- cuando se admite su utilización en organizaciones que se centran en el manejo de transacciones en línea, entre otras operaciones, no son aprovechados exhaustivamente en razón a que aún existe desconfianza a pesar de que se publicite la seguridad de las mismas [36].

Ante estas situaciones e innumerables inconvenientes presentados a cada momento con el uso del Internet, se pensaría en no utilizar la tecnología; pero desafortunadamente en nuestro medio y en estos momentos esa no es una opción posible: de una u otra manera se está obligado a hacerlo, máxime cuando las empresas que se quieren mantener activas deben ofrecer sus productos y servicios pues cada día es mayor la demanda de usuarios que utilizan la red para adquirir artículos y asistencia en línea. Y, a la vez, si quieren mantener un buen prestigio tecnológico deben prepararse para hacerlo; por lo que deben invertir para protegerse de diversas situaciones adversas y a la vez preservar el acceso de los posibles compradores que utilizan sus servicios [37]. De la misma manera, existen organizaciones de tipo comercial, que en aras de ofrecer sus productos utilizan estrategias consistentes en adelantar promociones en línea, las cuales son aprovechadas por los usuarios. Se ha encontrado que, como consecuencia, los sistemas empiezan a colapsar, generado descontento, pues se presenta mayor saturación del promedio en capacidad

[3]Ransomware. Es un tipo de malware que impide o limita los usuarios accedan a su sistema, ya sea mediante el bloqueo de la pantalla del sistema o mediante el bloqueo de los archivos de los usuarios, a menos que se pague un rescate. Más familias ransomware modernas, categorizadas colectivamente como cripto-ransomware, cifran ciertos tipos de archivos en los sistemas infectados y obliga a los usuarios a pagar el rescate a través de ciertos métodos de pago en línea para obtener una clave de descifrado.

de los servicios online. Para ello se sugiere la inversión en plataformas flexibles y escalables que pueden minimizar un sin número de riesgos relacionados con la seguridad, cuando la prestación de los servicios se hace basada en las redes sociales y la red informática mundial, entre otras [38].

Por lo hasta aquí expuesto, al respecto conviene advertir que es difícil e imposible confiar en Internet, pero aun así se sigue utilizando y cada día lo harán más usuarios y organizaciones. Es alarmante que para el primer trimestre de 2014, fueron afectados gran cantidad de dispositivos de conexión e interconexión y servidores en todo el mundo por la falla *bug Heartbleed*[4]; esto debido a que, como se dijo anteriormente, TCP/IP no es un protocolo seguro y el sistema operativo utiliza la librería OpenSSL vulnerable, la cual es utilizada para la protección criptográfica de datos compartidos entre clientes y servidores [39], obteniendo resultandos que hasta un 75 % de los usuarios de Internet tuvieron comprometidos sus datos de correo electrónico, redes sociales, aplicaciones de mensajería, sitios web, bancos y cajas de ahorro entre otras [40]. Así mismo, se desconoce desde hace cuántos años se haya venido interviniendo teléfonos, mensajes de voz, correos electrónicos, entre otros, y lo más sorprendente y complicado: sin saber si en algún momento pudo haber sido direccionado por hackers. Se puede decir que esta, la mayor falla en la seguridad de Internet en los últimos 12 doce años, es más agresiva pues no se detecta nada cuando el delito se ejecuta pues no deja pistas: "*se desconoce al ser hackeado*" [41].

3. Conclusiones

Es importante resaltar, a todo nivel, que las Organizaciones para poder mantenerse vigentes deben darse a conocer. La forma más económica y sencilla es a través de la red de redes, que se constituye en el medio masivo de consulta más fácil, económica y apropiada para la adquisición de diversidad de productos y servicios en el mundo. En la actualidad un alto porcentaje de usuarios consulta antes de tomar cualquier decisión, así nace la responsabilidad de proteger el activo más valioso para que las organizaciones puedan seguir funcionando: deben proteger su información de forma adecuada lo cual se logra con inversión.

De otra parte, es importante que las Organizaciones se estén continuamente modernizando tecnológicamente, sin descuidar la seguridad del activo más valioso invirtiendo, ya sea en tecnología o en capacitación. En muchas oportunidades ésta primera únicamente se instala y configura, pero no se le hace mantenimiento al sistema de forma continua, dejando a su paso vulnerabilidades que al ser descubiertas por intrusos afectan la correcta funcionalidad del sistema.

La constante aparición de tecnología hace cada vez más fácil el desarrollo de las actividades diarias de personas y organizaciones, esto hace posible la extensión y funcionalidad de las Instituciones desde dispositivos móviles, pero en este caso: ¿quién es el responsable?, pues intervienen diversos actores y factores tanto internos como externos; así se ve una vez más comprometida la seguridad informática. De igual manera, es recomendable con el fin de minimizar los riesgos, que los fabricantes de estos dispositivos sean los mismos que diseñen las aplicaciones que permiten conectarse a través de la red de redes, esto con el fin de minimizar los riesgos. No obstante, continúa la preocupación ya que una vez la información sale al exterior, ve comprometida su seguridad pues entra a formar parte de los espacios IP en los cuales la organización no puede vigilar y menos participar.

Ante tantas eventualidades presentadas en lo referente a la seguridad del activo más valioso, en las organizaciones se podría pensar en que una de las formas de minimizar los riesgos sería la evaluación a nivel interno de algunos ítems: administrativos, profesionales interdisciplinarios o de distintas disciplinas, tecnologías, aplicación de políticas, disponibilidad de recursos, capacitación, entre otros. Luego, la valoración de algunos de estos ítems frente a quienes prestan los servicios, con el fin de llegar a acuerdos, y desarrollar las actividades con el compromiso que atañe a cada uno de forma responsable en el momento apropiado, con los recursos y conocimientos suficientes; aunque en apariencia inviable y pensarlo utópico.

En la VII Encuesta Latinoamericana de Seguridad de la Información Nuevos retos, nuevas realidades, concluyó que la tendencia es que el área de seguridad de la información en las organizaciones se consolide, aunque su dependencia en el área de tecnología aún se mantenga. Producto de lo anterior, la visibilidad de los incidentes de seguridad de la información han aumentado la sensibilidad de las organizaciones sobre un adecuado tratamiento en la seguridad de la información. Desde esta perspectiva, algunas instituciones de educación superior, tanto nacionales como internacionales

[4] Grave vulnerabilidad en el popular OpenSSL biblioteca de software criptográfico. Esta debilidad permite robar la información protegida, bajo condiciones normales, por el cifrado SSL/TLS utilizado para asegurar la Internet. SSL/TLS proporciona seguridad de las comunicaciones y la privacidad a través de Internet para aplicaciones como web, correo electrónico, mensajería instantánea (IM) y algunas redes privadas virtuales (VPN).

han ofertado programas en seguridad informática, seguridad de la información, seguridad informática empresarial, seguridad de la información e Informática y ciberseguridad entre otros, pero es muy limitada la existencia programas suficientes y proyectos relacionados con investigación de temas relacionados, lo cual implica que programas posgraduales de especializaciones y de tipo de gestión ejecutiva sean implementados. Existen algunas temáticas que son muy importantes exhortar a la práctica sistemática de seguridad de la información: ciberseguridad, seguridad y control en la nube y fuga de información sensible, relacionados con la exposición de la información de las organizaciones. Asuntos como las monedas digitales[5]; internet de las cosas[6], entre otros elementos de vanguardia y de recientes desarrollos, demandarán acciones académicas y de desarrollo tecnológico para superar la incertidumbre que su implementación generará en las organizaciones y en la función de seguridad de la información.

Es decir, por más que se luche por la seguridad del activo más valioso de las organizaciones, siempre estará expuesta, justamente se tendrá que aceptar la convivencia con la inseguridad y al acecho de las organizaciones cibercriminales (Chaos Computer Club, TeaMp0isoN, The Level Seven Crew, LulzSec, The Network Crack Program Hacker Group, Anonymous y Milw0rm [42–47]), pero en sus justas proporciones y asumiendo el camino de la investigación, el desarrollo y la capacitación de manera crítica de alto nivel tecnológico y ejecutivo.

Referencias

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

[2] I. Chiavenato, "Introducción a la teoría general de la Administración", Séptima. ed México: Mc Graw Hill, 2006.

[3] C. A. B. Quirós, "EF el financiero". 28 de junio, 2016 [En línea] Disponible en: http://www.elfinancierocr.com/negocios/Comercio_Electronico-Correos_de_Costa_Rica-Ventas_en_linea_0_401959824.html

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

[5] D. Montero, "EF el financiero" 02 de marzo 2014. [En línea] Disponible en: http://www.elfinancierocr.com/economia-y-politica/Legales-David_Montero-seburidad_informatica_0_473352701.html

[6] RedUSERS, "La Voz". 27 de marzo, 2013. [En línea]. Disponible en: http://www.lavoz.com.ar/noticias/tecnologia/crean-mapa-con-maquinas-mas- vulnerables-mundo

[7] L. Diez Grajales, "Innovan en el Cuidado de Datos". 9 de junio 2010. [En línea] Disponible en: http://www.eluniversal.com.mx/finanzas/79909.html

[8] L. Custodio, "El País". 29 de julio 2013. [En línea] Disponible en http://www.elpais.com.uy/economia-y-mercado/desafio-invertir-seguridad-informatica- anadir.html

[9] Portafolio, "Cibercriminales", 20 de mayo, 2013. [En línea] Disponible en: http://www.portafolio.co/economia/finanzas/colombia-blanco-predilecto-cibercriminales- 58776

[10] Y. J. Mayorga, "Portafolio". 20 de diciembre 2012. [En línea] Disponible en: http://www.portafolio.co/economia/tecnologia-los-mas-pequenos

[11] N. Perlroth, "la La nación". 30 de marzo 2012. [En línea] Disponible en: http://www.lanacion.com.ar/1534880-las-pc-tambien-pueden-ser-blanco-de- secuestradores

[12] P. Cravero., "La Voz" 20 de noviembre 2012 [En línea] Disponible en: http://www.lavoz.com.ar/noticias/tecnologia/como-usar-redes-sociales-sin-ser-victima-delitos-informaticos

[13] M. R. Olvera, "El universal" 27 de abril 2012. [En línea] Disponible en: http://archivo.eluniversal.com.mx/finanzas/94688.html

[14] La. Nación, 31 de diciembre 2011. [En línea] Disponible en: http://www.lanacion.com.ar/1437007-redes-sociales-perdida-de-datos-y-sabotaje-desvelan-a-las-empresas

[5] Moneda digital o dinero digital. Es un medio de intercambio (es decir, distinto de físicos, como los billetes y monedas) que exhibe propiedades similares a las monedas físicas, sin embargo, permite las transacciones instantáneas y transferencia de propiedad sin fronteras [46].

[6] Internet de las cosas Internet de las cosas (IdC), 'Internet of Things (IoT)', 'Internet of Everything (IoE)'; como se le quiera denominar, el Internet en todo y para todos constituye la segunda gran revolución tecnológica después de la existencia misma de la Web, que ya está trayendo implicaciones en todos los campos de la vida económica, social y cultural [47].

[15] C. R. Vega, "Tecnología". 23 de abril 2012. [En línea] Disponible http://wvw.elfinancierocr.com/ef_archivo/2012/abril/29/tecnologia3149483.html?utm_source=newsletter&utm_medium=email&utm_campaign=2012-04-23

[16] I. Aigner, "Lainformacion.com". 05 de marzo 2012. [En línea] Disponible en: http://noticias.lainformacion.com/economia-negocios-y-finanzas/seguridad/encuesta-revela-vacios-en-seguridad-informatica-en-la-mayoria-de-las-empresas_bvaqpJeRwQn49zcnTNQBg7/

[17] V. M. Escamilla, "expansion". 16 de diciembre 2012 [En línea] Disponible en: http://www.cnnexpansion.com/mi-dinero/2011/12/14/compra-seguro-tus-regalos-por- internet

[18] C. Ruiz Vega, "EF El Financiero" 20 de enero 2014. [En línea] Disponible en: http://www.elfinancierocr.com/tecnologia/Hackers-supuesto-WhatsApp-distribuir-informatica_0_449955019.html

[19] C. R. VEGA, "El financiero" 16 de octubre 2012. [En línea] Disponible en: http://www.elfinancierocr.com/tecnologia/interrupcion-negocio-producto-ciberataque-cuesta_0_1733826663.html

[20] D. c. forensic, 2015. [En línea] Disponible http://www.delitosinformaticos.info/consejos/sobre_seguridad_informatica.html

[21] Portafolio, 08 de diciembre 2010. [En línea] Disponible http://m.portafolio.co/ciberdelincuentes-control-firmas/?tamano=grande

[22] E. Fernandez, "Seguridad de las Tecnologías de la información. La construcción de la confianza para una sociedad conectada", España: Ediciones AENOR, 2003.

[23] J. J. C. M., "Computación forense descubriendo los rastros informáticos", Primera. ed., México: Alfa omega Grupo Editor, S.A. de C.V, 2009.

[24] J. Carretero, "sistemas Sistemas operativos Una Visión aplicada", México: Mc Graw Hill, 2007.

[25] TechNet, 08 mayo 2012. [En línea] Disponible en: https://technet.microsoft.com/library/security/ms12-032

[26] T. d. seguridad, 12 abril 2005. [En línea] Disponible https://www.microsoft.com/latam/technet/seguridad/boletines/ms05-019.mspx

[27] M. TechNet, 08 septiembre 2009. [En línea]. Disponible en: https://www.microsoft.com/latam/technet/seguridad/boletines/2009/ms09-048.mspx

[28] M. TechNet, 11 noviembre 2014. [En línea]. Disponible en: https://technet.microsoft.com/es-es/library/security/ms14-070

[29] J. e. I. Tecnología, 12 agosto 2016. [En línea] Disponible en: https://www.meneame.net/m/tecnolog%C3%ADa/search?p=tags&q=cve-2016-5696

[30] F. CATOIRA, "Wilivesecurity". 20 marzo 2012. [En línea] Disponible http://www.welivesecurity.com/la-es/2012/03/20/grave-vulnerabilidad-ms12-020- sistemas-microsoft/

[31] J. Cano, "ACIS". 2013. [En línea] Disponible en: http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/XIII_JornadaSeguridad/EL SI2013.pdf

[32] J. Cano, "ACIS". Junio 2016. [En línea] Disponible en: http://acis.org.co/archivos/JornadaSeguridad/ENCUESTA %20LATINOAMERICANA.pdf

[33] M. Prieto, "SmartLIGHTING". 14 marzo 2017. [En línea] Disponible en: http://smart-lighting.es/ransomware-incremento-informe-anual-seguridad-trend-micro/

[34] Symantec, junio 2014. [En línea] Disponible en: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

[35] N. Jodal, "El Financiero". 02 octubre, 2013. [En línea] Disponible en: http://www.elfinancierocr.com/tecnologia/seguridad-Internet-imposible-advierte-experto_0_383961621.html

[36] Portafolio, 20 noviembre, 2013. [En línea] Disponible en: http://www.portafolio.co/negocios/los-usuarios-internet-aun-desconfian-la-banca-linea

[37] E. Financiero, 27 noviembre, 2012. [En línea] Disponible en: http://www.elfinancierocr.com/pymes/medidas-mantener-seguro-sitio-empresa_0_207579792.html

[38] R. Rivera, "emol.economia". 25 noviembre, 2012. [En línea] Disponible en: http://www.emol.com/noticias/economia/2012/11/23/571122/cyber-monday-estan-preparadas-nuestras-redes-para-esta-fiesta-del-consumo.html

[39] J. A. R. Franco, "Evaluación desde la óptica de la computación forense del BUG". *Revista Ingeniería, Matemáticas y Ciencias de la Información*, vol. 2, no. 4, p. 103, 2015.

[40] TeknoPLOF, 13 mayo, 2016. [En línea] Disponible en: http://www.teknoplof.com/tag/bug/

[41] J. Pagliery, "expansion". 14 abril 2014. [En línea] Disponible en: http://expansion.mx/tecnologia/2014/04/14/heartbleed-tambien-afecta-a-gadgets

[42] Altonivel, 16 de mayo 2017. [En línea] Disponible en: http://www.altonivel.com.mx/los-hackers-mas-famosos-del-mundo/

[43] EcuRed, "informática forense" 13 de marzo de 2016. [En línea] Disponible en: https://www.ecured.cu/Inform %C3 %A1tica_Forense

[44] TrendMicro "Ransomware" 23 de marzo de 2016. [En línea] Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[45] "El insecto de Heartbleed", 30 de marzo de 2016. [En línea] Disponible en: http://translate.google.com.co/translate?hl=es&sl=en&u=http://heartbleed.com/&prev=/search %3Fq %3DHeartbleed %26biw %3D1280 %26bih %3D656

[46] "Moneda digital" 02 de abril de 2016. [En línea] Disponible en: http://copro.com.ar/Moneda_digital.html

[47] Colombia Digital, "el internet de las cosas" 30 de marzo de 2016. [En línea] Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/7821- internet-de-las-cosas-concepto-y-ecosistema.html