Artículo Original

Una forma de interpretar la seguridad informática

Diana Suárez[1], Aldeir Ávila Fontalvo[2]

Artículo recibido: 10 de septiembre de 2013 / Artículo aceptado: 12 de diciembre de 2013

RESUMEN

La seguridad informática actualmente forma parte de los grandes negocios en materia de tecnología y seguridad en las empresas. Debido a que hoy en día se reflejan distintos tipos de ataques y amenazas al acceso de la información de las organizaciones, es necesario crear medidas y procesos que contrarresten estos peligros que afectan los recursos funcionales de las entidades. Por eso, se requiere la disposición de diferentes mecanismos de seguridad que van relacionados con varios tipos de recursos tanto humanos como tecnológicos que ayudan a garantizar una muy buena seguridad en las empresas. El recurso humano entonces, se convierte en un elemento fundamental a la hora de definir pautas de seguridad que garanticen la robustez de un sistema de información. La seguridad de la información es un tema de nunca acabar y que por tal motivo la actualización de los distintos recursos y procesos que se identifiquen día a día es sumamente importante para minimizar los riesgos en el ámbito de seguridad de las organizaciones.

Palabras clave: seguridad, información, mecanismos, recursos, tecnología.

1 Ingeniera de Sistemas. Docente de la Universidad Simón Bolívar. dsuarez@unisimonbolivar.edu.co
2 Estudiante de 9° semestre de Ingeniería de Sistemas, Corporación Universitaria Americana. Aldeavi04@hotmail.com
Autor para correspondencia: dsuarez@unisimonbolivar.edu.co

A way for interpreting technology security

ABSTRACT

Due different types of assaults and threats to access information of organizations reflected nowadays, measures and processes are adopted to counteract these dangers which affect functional resources of the entities taking into account that technology security (technology and security) is part of a big business. Different available mechanisms of safety related to several types of both human and technological resources that guarantee a good safety for companies is required. Then, human resources turn into a main element when safety guidelines which guarantee the resilience of data system are defined. The safety of information turns into never ending story, that is why, the updated different resources and processes identified day after day are extremely important to minimize the risks in organizations' safety area.

Keywords: security, information, mechanism, resources, technology.

Uma forma de interpretar a segurança informática

RESUMO

A segurança informática atualmente forma parte dos grandes negócios em matéria de tecnologia e segurança nas empresas. Devido a que hoje em dia se reflete distintos tipos de ataques e ameaças ao acesso da informação das organizações, é necessário criar medidas e processos que contrabalancem estes perigos que afetam os recursos funcionais das entidades. Por isso, se requere a disposição de diferentes mecanismos de segurança que vão relacionados com vários tipos de recursos tanto humanos como tecnológicos que ajudam a garantir uma muito boa segurança nas empresas. O recurso humano então, se converte em um elemento fundamental na hora de definir pautas de segurança que garantem a robustez de um sistema de informação. A segurança da informação é um assunto de nunca acabar e que por tal motivo a atualização dos diferentes recursos e processos que se identifiquem dia a dia é sumamente importante para minimizar os riscos no âmbito de segurança das organizações.

Palavras chave: segurança, informação, mecanismos, recursos, tecnologia.

INTRODUCCIÓN

Actualmente las grandes y pequeñas empresas, locales, entidades y todo tipo de negocios que administran distintos tipos de recursos como son la información y equipos de cómputo encaminados a conexiones de redes buscan la necesidad de hacer que su sistema sea más robusto y estable en materia de seguridad.

La seguridad informática se enfoca en la protección de los recursos tecnológicos como los equipos de cómputo, servidores, routers, cables, etc. y, especialmente, la información contenida o circulante. Para ello, existen una

serie de procesos y utilidades determinadas para reducir los posibles peligros al área física de la organización o a la información. La seguridad informática comprende lo lógico (bases de datos, información), hardware (computadores, servidores, impresoras, entre otros) y todo lo que la entidad considere de mucha importancia y signifique una alarma si esta información pasa a manos de otros sujetos, convirtiéndose, por ejemplo, en información privada [1].

La seguridad informática hoy en día se ha convertido en uno de los grandes negocios en el mercado, ya que ingenieros, técnicos, especialistas en el tema y otros desarrollan todo tipo de métodos y procedimientos que ayudan a reforzar o mantener un sistema "seguro".

Su principal característica es la confidencialidad de la información que es entonces, lo que se quiere proteger y salvaguardar de personas que no estén autorizadas para consultar en el sistema cualquier dato, que pueda convertirse en una vulnerabilidad para poder acceder a este.

Un sistema requiere de seguridad en todo momento por lo cual actualizar los métodos, normas y pautas de seguridad en una entidad es sumamente importante y por ende, esto tiene un ciclo que no puede terminar de un día para otro, ya que si algún momento, la organización deja de ser segura, se convierte en un blanco para aquellas personas que buscan con fines maliciosos alterar y robar la información del sistema.

Con base en lo anterior si hablamos de seguridad informática, su concepto, su estado, sus características u otro aspecto, nos preguntamos:

¿qué es lo que buscan las empresas u organizaciones en seguridad? ¿Qué aspectos a tener en cuenta se evalúan para mantener o conversar un sistema seguro? ¿Qué tipo de amenazas hacen que un sistema no sea seguro? En análisis a estas preguntas se tocan tres aspectos a analizar a continuación:

1. Recurso humano o tecnológico o ambos en función de seguridad informática.

2. Características, mecanismos, recursos y normas para garantizar un sistema seguro.

3. Ataques y amenazas a una organización.

DESARROLLO

Los recursos humanos son todas aquellas personas que hacen parte del ámbito organizacional y que de ellas depende la buena administración de la seguridad de la información en la empresa. La información es manejada adecuadamente siempre y cuando se gestione por personal asignado para esta gestión, por tanto, no se puede asegurar la confidencialidad de la información sin un buen papel en sus oficios de los recursos humanos [2].

Proteger los activos de información con los que cuenta la organización no es una tarea de un solo departamento, sino que debe ser compartida por toda la empresa, dividiéndose cada módulo de esta, la información o conjunto de datos específicos para que cada área se relacione adecuadamente en el tráfico de datos y así funcione muy bien la entidad.

Cada módulo juega un papel fundamental en la información y por ende, cada uno de ellos cumple una función específica que permite gestionar todos los procesos de la empresa teniendo en cuenta la normatividad que se debe cumplir de acuerdo con el reglamento de la organización.

Un recurso tecnológico puede ser un objeto, herramienta o guía que se relaciona bastante con el concepto de tecnología (conocimientos y procesos) para cumplir un objetivo. En este caso los recursos tecnológicos ayudan a las empresas a gestionar sus procesos, tareas e información para garantizar el éxito de la misma con la venta de sus productos [3].

Los recursos tecnológicos pueden ser físicos o lógicos, siendo los físicos: un computador, una impresora u otra máquina; y los lógicos: una aplicación, un software virtual, etc. Estos recursos varían dependiendo del objetivo de la organización [4].

Cabe destacar que los recursos tecnológicos lógicos son fundamentales, a la hora de establecer comunicación con los clientes, de manera que así se den a conocer cada uno de los servicios que la entidad brinda a la comunidad. Sin embargo, no solo hay comunicación con los clientes, también estos, permiten entablar conexión con los mismos empleados de la empresa o distintos usuarios que tienen permisos específicos para manipular la información dentro de esta.

Los recursos humanos y tecnológicos son el pilar más importante dentro de una empresa, ya que sin estos, no se podría gestionar una correcta manipulación de su información. Combinar estos dos recursos significa garantizar que se puede establecer un sistema empresarial capaz de administrar procesos que ayuden a la satisfacción de los clientes en un servicio o producto específico.

Dentro del ámbito de seguridad, el personal dedicado a esta área en la empresa deben ser personas capacitadas, con certificaciones en alguna entidad que garantice que estos pueden brindar el servicio de seguridad en una organización, cumpliendo los estándares que indiquen el grado de seguridad que estos pueden brindar a las empresas. Entre más haya personal capacitado en esta área, más se verá reflejado una buena seguridad física en la organización.

Con respecto a seguridad con equipos de cómputo, tecnologías de autenticación, control de acceso, sistemas de información, software de desarrollo y todos aquellos recursos tecnológicos que gestionen la información, desarrollo, procesos y acceso deben ser en lo posible de última tecnología, que no sean tan vulnerables a personas no autorizadas, que los software cuenten con licencia, que los controles y tecnologías de acceso al sistema y a los módulos de la empresa funcionen correctamente, que cada uno de estos recursos se utilice en el momento indicado, que cuenten con estándares de calidad.

Tanto los recursos tecnológicos y humanos entre más actualizados estén en concepto de normatividad, pautas, tecnología, versiones y funciones mejor funcionará la seguridad de la empresa, debido a que la organización estaría al tanto de todas las innovaciones, procesos y mecanismos que cada día saltan al mercado. Una correcta gestión de recursos humanos y tecnológicos garantiza seguridad de la información y demás en una organización.

Para garantizar la seguridad en una organización es necesario establecer una serie de mecanismos que actúen en función de los recursos, normas y características con que cuenta la empresa. Aquí influyen mucho los recursos tecnológicos y humanos, mencionados anteriormente ya que estos son el eje principal para no dejar en riesgo la información y demás activos de la entidad.

Se debe tener en cuenta la clasificación de estos mecanismos de seguridad, ya que no se debe confundir un procedimiento o mecanismo con otro, debido a que más de uno de estos, utilizan el mismo recurso tecnológico o humano y por lo tanto, se deben estructurar, es decir crear reglas o normas que indiquen su debido uso que pueden ser según su clasificación preventivos, detectivos y correctivos [5].

Cada uno de estos, cumplen una función distinta y se utilizan en un momento determinado, por ejemplo, el preventivo tiene la función de avisar al sistema, antes de que un peligroso proceso o hecho no deseado lo afecte directamente. El detectivo identifica y avisa algún evento no autorizado y lo registra en el sistema. Y el correctivo, corrige la secuencia de errores o posibles procesos que están presentando alguna anomalía en la organización [6].

En general existen a nivel comercial muchas herramientas o técnicas que ayudan a mantener un sistema seguro, dependiendo del tipo de acceso al sistema o a los diferentes módulos con que cuenta la organización, como por ejemplo, el acceso físico a la entidad, el acceso a los equipos de cómputo en un módulo, las bases de datos, los servidores, los software de desarrollo de trabajo de la empresa, todos estos son un blanco para las personas con objetivos de tumbar el sistema y su estructura.

Tales herramientas o técnicas son huella digital, verificación de voz, verificación de patrones oculares, contraseñas, claves encriptadas, *firewall*, restricciones, simetría, cifrados, protocolos se seguridad, autenticación a nivel de software, antivirus y en general una gran variedad de herramientas que inciden en el sistema para mantenerlo seguro [7].

El autor considera que este tipo de herramientas y procedimientos de una u otra forma ayudan al control de la seguridad en una organización, pero no convierten un sistema totalmente seguro. Puede que estas ofrezcan numerosas posibilidades de establecer un sistema robusto y libre de muchos ataques, pero no garantizan la total seguridad de este, ya que siempre se debe tener presente que cada día se inventan más y más formas de atacar o vulnerar un sistema, entonces, las entidades deben pensar más en actualizarse en este tipo de temas tan importantes como lo es la seguridad, para enfocarse más en las nuevas tecnologías que ayudan a contraatacar estas amenazas. Si un sistema no cuenta con normas de seguridad establecidas por alguna ISO u otra organización, tecnologías de última generación, de todas formas siempre va estar expuesto a cualquier ataque en algún momento. En conclusión entre más se minimice el riesgo de ser atacado, mejor será su sistema en el tema de seguridad.

Para Borghello, los ataques y amenazas a una organización se identifican debido al tipo de acceso al sistema, la forma en que operan quienes intentan realizar estos procesos y los objetivos que estos quieren

alcanzar. Un atacante es cualquier persona que utiliza un medio específico y con conjunto de herramientas para intentar acceder a un sistema y manipular la información almacenada en este [8].

Los ataques informáticos se registran desde muchos años atrás y con el paso del tiempo se han vuelto más robustos y difíciles de identificar debido a los procesos y tipos de herramientas desarrolladas por los atacantes, quienes como objetivo buscan acceder a un sistema por todos los medios posibles [9].

Sin embargo, hasta el que no es un experto en temas de *hacking* informático o desarrollo de software malicioso, solo con una eficaz herramienta informática lógica o física capaz de ser manipulada por este, puede alterar un sistema en cuestión de horas, minutos o segundos dependiendo de la seguridad que este tenga [10].

Para la Universidad Nacional de Lujan, una amenaza es todo objeto o sujeto o proceso capaz de atacar contra la seguridad de los datos de una organización y estas se originan a partir de la existencia de huecos o fallas en lo referente al hardware o software de la empresa, por esta razón, este concepto está directamente relacionado con el de ataques, ya que un atacante aprovecha estas vulnerabilidades (si existen en el sistema) o investiga que módulo o características específicas del sistema pueden ser vulnerables para atacar por esa "brecha" a este y poder acceder a la información [11].

Estas amenazas pueden ser intencionales o no intencionales. Las no intencionales se pueden presentar hasta en la misma organización, cuando un miembro de esta puede cometer una falla o error que haga que el sistema se encuentre en riesgo de ser atacado por personas extrañas. Y las intencionales son aquellas en las que por ejemplo algún hacker intenta atacar el sistema con distintos métodos [12].

Existen muchos tipos de ataques, que atentan contra los recursos humanos, tecnológicos y de la información en una empresa, tales como ingeniería social, ingeniería social inversa, *trashing*, ataques de monitorización, ataques de autenticación, *Denial of Service*, ataques de modificación, etc., todos con el fin de atacar algún modulo específico de la organización [13].

Hoy en día los ataques son muy frecuentes, en cualquier tipo de organización. Nadie está exento de sufrir un ataque informático, por eso, es necesario la implementación de técnicas y mecanismos como los mencionados anteriormente para reducir el riesgo del sistema y sobre todo ponerse al tanto de las actualizaciones que ofrecen las empresas en este tipo de mecanismos y procedimientos y también del tipo de ataques que surgen cada día.

Es importante evitar que la organización reciba algún ataque que afecte tanto a la información como a lo financiero, ya que se podrían producir pérdidas que se recuperarían a largo plazo siempre y cuando se tomen las medidas necesarias para restablecer el sistema. Siempre se debe tener presente que la seguridad es un aspecto que no puede olvidarse, porque esta es la base de todas las organizaciones, si no hay seguridad, no habrá integridad, confidencialidad o disponibilidad en todo momento en la empresa y eso sería

un aspecto muy grave a evaluar para mejorar la eficacia de los procesos de la organización.

CONCLUSIONES

Para concluir, hay que tener en cuenta que la seguridad informática es proceso dinámico, es decir, suele siempre estar encaminado a la actualización permanente de mecanismos, métodos, técnicas y procedimientos que ayudan a contrarrestar los ataques o amenazas informáticas que también cada día aparecen en Internet, redes y demás medios en donde puedan realizar sus procedimientos con objetivos determinados.

Un sistema no está 100 % seguro en ningún momento, y está siempre al alcance de ser atacado por cualquier virus, proceso o persona que quiera lograr robar o manipular información de una organización, así que, ninguna persona, especialista, entidad u otro puede decir que mantiene su sistema en su total protección.

En relación con la protección de los datos y recursos que se relacionan para lograr los objetivos de una empresa siempre se deben tener actualizados con las últimas tendencias en el mercado en cuestión de seguridad informática, ya que así, se garantiza que el sistema tenga un grado de seguridad bueno y permanente que permita manipular con tranquilidad los procesos que llevan a cabo las organizaciones para cumplir sus metas.

Los recursos tecnológicos y humanos y los mecanismos y distintas técnicas que existen para mantener un sistema seguro deben ser elementos rígidos dentro de una organización, es decir, no deben ser tan vulnerables a ataques informáticos, por lo tanto, siempre hay que consultar, analizar y evaluar qué elementos de seguridad nos proporcionan una debida protección dependiendo del tipo de funcionamiento que maneje una empresa.

También hay que tener presente, que no siempre los ataques a los sistemas se producen por parte de personas extrañas o que no pertenecen a una organización, actualmente la mayoría de estos ataques, son hechos por personas de la misma empresa, siendo estas las principales promotoras de dejar en un estado de riesgo a los procesos de la entidad.

La seguridad informática es muy importante en muchos campos y organizaciones de la sociedad y para garantizar que esta sea posible de manera exitosa, se debe investigar y evaluar qué herramientas nos brindan actualmente los mercados expertos en este tema y así poder establecerlas, en la organización, de modo que cada miembro de la empresa tenga presente el grado de importancia que representa la seguridad informática en los sistemas.

REFERENCIAS

[1] S. Arcos y M. Ribera Sancho, *Psicología aplicada a la seguridad informática Samsó*, 2011. Recuperado en http:// es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

[2] E. Gracia, J. León, y N. Del Cid, *Seguridad de la información en los Re cursos Humanos,* 2010. Recuperado en http://es.slideshare.net/123jou/ seguridad-de-la-informacion-en-los-recursos-humanos.

[3],[4] *Definición de recursos tecnológicos,* 2014. Recuperado en http://definicion. de/recursos-tecnologicos/

[5], [6], [7] J. Ríos, *Seguridad informática*, 2014. Recuperado en http://www.monografias.com/trabajos82/la-seguridad-in-formatica/la-seguridad-informatica2.shtml#mecanismoa#ixzz3GPpvcb9j

[8], [9], [10], [13] C. Borghello, *Amenazas lógicas - Tipos de ataques*, 2009. Recuperado en el 2008-2009, en http://www. segu-info.com.ar/ataques/ataques.htm

[11], [12] Universidad Nacional de Lujan (s.f.), *Amenazas a la seguridad de la información*, Buenos Aires, Argentina. Recuperado en http://www.seguridadinformatica.unlu.edu.ar/?q=node/12