Dom. Cien., ISSN: 2477-8818
Vol. 3, núm. 5, julio, 2017, pp. 676-688

Número Publicado el 26 de Agosto de 2017

http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688
URL:http://dominiodelasciencias.com/ojs/index.php/es/index

Ciencias Informáticas

Artículo Corto

Seguridad en informática: consideraciones

Computer security: considerations

Silvia M. Quiroz-Zambrano [I]
Universidad Laica Eloy Alfaro de Manabí
mabelquirozz@gmail.com

David G. Macías-Valencia [II]
Universidad Laica Eloy Alfaro de Manabí
davmacval68@gmail.com

Recibido: 30 de enero de 2017 ***** **Corregido:** 20 de febrero de 2017 ***** **Aceptado:** 20 junio de 2017

I. Ingeniera en Sistemas Informáticos, Tecnólogo en Computación Administrativa, Docente de la Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador en Sistemas, Universidad Laica Eloy Alfaro de Manabí.
II. Universidad Laica Eloy Alfaro de Manabí.

Resumen

La globalización de la economía ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. Se realizó una revisión bibliográfica en la cual se expone en el trabajo los riesgos, amenazas vulnerabilidades, que afectan a esa información y por ende al sistema.

Palabras clave: Seguridad informática; riesgo; amenazas.

Abstract

The globalization of the economy has required companies to implement technological platforms that support the new way of doing business. The use of the Internet for this purpose, entails the development of computer security projects that guarantee the integrity, availability and accessibility of information. A bibliographic review was carried out in which the risks, threats and vulnerabilities that affect this information and, therefore, the system are exposed in the work.

Key words: Informatic security; risk; threats.

Introducción.

El ambiente de los *sistemas de información* que predominó hasta principios de la década de los noventa, –previo a la globalización de las telecomunicaciones, las redes mundiales de teleproceso, la *Internet*, etcétera– tuvo como una de sus características más relevantes la de poseer entornos informáticos en los que se operaba de manera aislada o en redes privadas en las cuales, la seguridad impuesta por el acceso físico y algunas simples barreras informáticas bastaban para que la seguridad de la información en ellos contenida estuviese garantizada. Por lo mismo, no había mucha preocupación al respecto ni estrategias al efecto. En 1977, el senador Abraham A. Ribicoff, de Connecticut, EUA, propuso una iniciativa de "Acta de Ptotección de los Sistemas de Cómputo Federales", la cual buscaba por primera vez definir cibercrímenes y recomendar sanciones por dichos delitos. La iniciativa no prosperó en esa ocasión.((Voutssas M., J. 2010), (Timeline: The US Government and Cybersecurity". 2003)

En ese mismo sentido, en la actualidad, los sistemas de información han sido sustituidos casi en su totalidad por Tecnologías de Información y Comunicaciones (TIC) convergentes, por inmensas y cada vez más complejas redes institucionales locales y regionales, por servidores y computadoras personales que cada vez tienen mayor capacidad de proceso y de acceso a otros computadores, y cuya interconexión se extiende mundialmente. Al mismo tiempo, la *Internet* forma ya parte de la infraestructura operativa de sectores estratégicos de todos los países como el comercial, energía, transportes, banca y finanzas, –por mencionar algunos– y desempeña un papel fundamental en la forma en que los gobiernos proporcionan sus servicios e interactúan con organizaciones, empresas y ciudadanía, y es un factor cada vez más creciente de intercambio de

información de manera individual por parte de los ciudadanos toda vez que se forman redes sociales cada vez más complejas. (Voutssas M., J. 2010)

La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también han cambiado de manera significativa. El número y tipo de dispositivos, servicios y variedades que integran la infraestructura de acceso se ha multiplicado, e incluye ya variados elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente. Como consecuencia de todos estos cambios el volumen, naturaleza, disponibilidad y sensibilidad de la información que se intercambia a través de esta infraestructura se ha modificado y ha aumentado de manera muy significativa. (Voutssas M., J. 2010).

El mundo digital se ha integrado en toda la sociedad de una forma vertiginosa, en nuestro diario vivir son más las personas que se apoyan en Internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre ip, descargar música o el libro favorito, hacer publicidad, etc. Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas. Las “transacciones” electrónicas nos permiten ahorrar tiempo y recursos, pagar los servicios públicos, transferir de una cuenta bancaria a otra, participar en una subasta para comprar un vehículo, pagar un boleto de avión etc. En todos estos ejemplos hay algo en común, el dinero, y cuando hablamos de tan escaso pero tan apreciado bien las empresas deben garantizar la implementación de políticas de seguridad informática. (Dussan Clavijo, C A. 2006)

Conceptos fundamentales de la seguridad informática:

Voutssas M., J (2010) expone en su artículo que para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen, ya que de otra forma no es posible establecer una base de estudio. Los enunciaré a continuación y los desarrollaré con más detalle más adelante.

Recursos Informáticos: el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como "activos informáticos"

Amenaza: fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.

Impacto: la medida del efecto nocivo de un evento.

Vulnerabilidad: característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.

Riesgo: la probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.

Principio básico de la seguridad informática: la seguridad informática no es un producto, es un proceso.

El objetivo primario de la *seguridad informática* es el de mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo

aceptable. Para ello utilizaremos estructuras organizacionales técnicas, administrativas, gerenciales o legales.

El objetivo secundario de la *seguridad informática –y* subrayo que es de nuestro especial interés desde el punto de vista de la preservación documental– consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total. Este concepto varía de acuerdo a distintos autores, a los contextos documentales y al tipo de organización a la que la información esté asociada. En un contexto archivístico y en donde tratamos de interoperar un enfoque de seguridad informática con uno de preservación digital, podemos establecer esa confiabilidad como la unión de seis características esenciales:

- permanencia
- accesibilidad
- disponibilidad
- confidencialidad (privacidad)
- autenticidad (integridad)
- aceptabilidad (no repudio)

Amenazas informática.

Los primeros virus informáticos surgieron como experimentos en universidades, juegos, o simplemente con el propósito de molestar, pero no directamente con el objetivo de causar daños en los equipos informáticos.

Así los primeros virus datan de los años 70, cuando el uso de ordenadores no era popular. El primer virus conocido fue el Creeper (enredadera), que simplemente sacaba repetidamente por pantalla el siguiente mensaje "¡Soy una enredadera... agárrame si puedes!" Para combatirlo se creó el primer antivirus, llamado Reaper (cortadora).

En la actualidad la propagación del malware resulta mucho más rápida, sobre todo gracias al uso de internet. Además ahora los virus no buscan en la mayoría de los casos la notoriedad, si no más bien todo lo contrario: permanecer ocultos en el sistema sin que la persona usuaria sepa que su ordenador está infectado.

Por otro lado ya no tienen sólo como objetivo dañar el sistema, si no que pueden sustraer información sensible del equipo informático (contraseñas, números de tarjetas de crédito, etc...) o utilizar el equipo para realizar ataques a otros sistemas a través de él.(Amenazas informáticas. 2015)

De acuerdo con los razonamientos que se han venido realizando las amenazas, como ya hemos mencionado, consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma. Entre ellas, identificamos como las principales:

El advenimiento y proliferación de "malware" o "malicious software", programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.

La pérdida, destrucción, alteración, o sustracción de información por parte de personal de la organización debido a negligencia, dolo, mala capacitación, falta de responsabilidad laboral, mal uso, ignorancia, apagado o elusión de dispositivos de seguridad y/o buenas prácticas.

La pérdida, destrucción, alteración, sustracción, consulta y divulgación de información por parte de personas o grupos externos malintencionados.

El acceso no autorizado a conjuntos de información.

La pérdida, destrucción o sustracción de información debida a vandalismo.

Los ataques de negación de servicio o de intrusión a los sistemas de la organización por parte de ciber–criminales: personas o grupos malintencionados quienes apoyan o realizan actividades criminales y que usan estos ataques o amenazan con usarlos, como medios de presión o extorsión.

Los "phishers", especializados en robo de identidades personales y otros ataques del tipo de "ingeniería social".

Los "spammers" y otros mercadotecnistas irresponsables y egoístas quienes saturan y desperdician el ancho de banda de las organizaciones.

La pérdida o destrucción de información debida a accidentes y fallas del equipo: fallas de energía, fallas debidas a calentamiento, aterrizamiento, desmagnetización, rayadura o descompostura de dispositivos de almacenamiento, etcétera.

La pérdida o destrucción de información debida a catástrofes naturales: inundaciones, tormentas, incendios, sismos, etcétera.

El advenimiento de tecnologías avanzadas tales como el cómputo *quantum*, mismas que pueden ser utilizadas para desencriptar documentos, llaves, etcétera al combinar complejos principios físicos, matemáticos y computacionales. (Granger S . 2009)

Vulnerabilidades informáticas.

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas. Podemos diferenciar tres tipos de vulnerabilidades según cómo afectan a nuestro sistema:

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrallan el programa al que afecta y para las cuales ya existe una solución, que se publica en forma de parche. Existen listas de correo relacionadas con las noticias oficiales de seguridad que informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos.

Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este pragrama. Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. Esto ha llevado a que empresas como Microsoft dispongan de departamentos dedicados

exclusivamente a la seguridad, como es Microsoft Security Response Center (MSRC). Sus funciones son, entre otras, evaluar los informes que los clientes proporcionan sobre posibles vulnerabilidades en sus productos, y preparar y divulgar revisiones y boletines de seguridad que respondan a estos informes.

Para ello clasifica las vulnerabilidades en función de su gravedad, lo que nos da una idea de los efectos que pueden tener en los sistemas: criticas , importantes , moderadas y bajas . (Seguridad informática .2013)

Riesgos informáticos.

El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza. .(Santana Roldan C . 2012)

El riesgo se utiliza sobre todo el análisis de riesgos de un sistema informático. Esté riesgo permite tomar decisiones para proteger mejor al sistema. Se puede comparar con el riesgo límite que acepte para su equipo, de tal forma que si el riesgo calculado es inferior al de referencia, éste se convierte en un riesgo residual que podemos considerar cómo riesgo aceptable. (Santana Roldan C. 2012)

Según Voutssas M , J (2010), define el riesgo como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto.

Impactos

Los impactos son los efectos nocivos contra la información de la organización al materializarse una amenaza informática. Al suceder incidentes contra la seguridad informática pueden devenir en:

Disrupción en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa.

Pérdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, público en general, medios de información, etcétera.

Costo político y social derivado de la divulgación de incidentes en la seguridad informática.

Violación por parte de la organización a la normatividad acerca de confidencialidad y privacidad de datos de las personas.

Multas, sanciones o fincado de responsabilidades por violaciones a normatividad de confidencialidad.

Pérdida de la privacidad en registros y documentos de personas.

Pérdida de confianza en las tecnologías de información por parte del personal de la organización y del público en general.

Incremento sensible y no programado en gastos emergentes de seguridad.

Costos de reemplazo de equipos, programas, y otros activos informáticos dañados, robados, perdidos o corrompidos en incidentes de seguridad . (Voutssas M., J 2010)

Actuaciones para mejorar la seguridad

Los pasos a seguir para mejorar la seguridad son los siguientes:

Identificar los activos, es decir, los elementos que la empresa quiere proteger.

Formación de los trabajadores de las empresas en cuanto a materias de seguridad.

Concienciación de la importancia de la seguridad informática para los trabajadores de la empresa.

Evaluar los riesgos, considerando el impacto que pueden tener los daños que se produzcan sobre los activos y las vulnerabilidades del sistema.

Diseñar el plan de actuación, que debe incluir:

a) Las medidas que traten de minimizar el impacto de los daños ya producidos. Es lo que hemos estudiado referido a la seguridad pasiva.
b) Las medidos que traten de prevenir los daños minimizando la existencia de vulnerabilidades. Se trata de la seguridad activa.

b) Revisar periódicamente las medidas de seguridad adoptadas

Acciones de "ingeniería social" malintencionada: "phishing", "spam", espionaje, etcétera.

Uso indebido de materiales sujetos a derechos de propiedad intelectual.

Daño físico a instalaciones, equipos, programas, etcétera.

Finalmente la seguridad informática pretende identificar las amenzas y reducir los riesgos al detectar las vulnerabilidades nulificando o minimizando así el impacto o efecto nocivo sobre la

organización. Si analizamos y juntamos todo lo anterior creo que estamos ya en posibilidad de comprender por qué la "seguridad informática" se definió entonces como "el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos".

Referencia bibliográfica.

Amenazas informáticas. [sitio web]. 2015 [consulta 25 enero 2017]. Disponible en : forma.kzgunea.eus/mod/book/view.php?id=5800&chapterid=7518

DUSSAN CLAVIJO, C A. 2006. Políticas de seguridad informática Entramado, 2 (1),, pp. 86-92 Universidad Libre Cali, Colombia. Disponible en: http://www.redalyc.org/articulo.oa?id=265420388008

GRANGER S . 2009. "Social Engineering Fundamentals, Part I: Hacker Tactics". Security Focus. [consulta 11 enero 2017] Disponible, en: http://www.securityfocus.com/infocus/1527

Seguridad informática [sitio web]. 2013. [consulta 25 enero 2017]. Disponible en : https://infosegur.wordpress.com/tag/vulnerabilidades/

SANTANA ROLDAN C. 2012. Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? [consulta 25 enero 2017]. Disponible en. https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

VOUTSSAS M., Juan. 2010. Preservación documental digital y seguridad informática. *Investig. bibl* 24(50)., pp.127-155. ISSN 2448-8321.Disponible en: <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&nrm=iso>.

Timeline: The US Government and Cybersecurity"[sitio web]. 2003. Compiled by *The Washington Post.2009* [consulta 11 enero 2017] Disponible en: http://www.washingtonpost.com/wp–dyn/articles/A50606–2002Jun26.html