SEGURIDAD INFORMÁTICA, IMPORTANCIA DESDE LA PERSPECTIVA DEL RECURSO HUMANO

Vargas Jenny, López Pablo.
jenina06@gmail.com, palspab@gmail.com
Universidad Piloto de Colombia
Bogotá, Colombia

Abstract— With the changes in current trends, which are oriented towards information technology, care of data has become increasingly important, so much so that the information today is considered an asset in the organization, this reason, this document expresses the importance of keeping information secure, how to Generate a safety culture within the company and how that culture should be handled and transplanted workers within an organization.

Throughout the document elements that support the importance of strengthening the security of business information and generate a tool for raising awareness of the human resources of an organization for the conservation of information in secure environments are presented.

Keywords: Information, Security, Safety Culture, Privacy

Resumen— Con los cambios en las tendencias actuales, las cuales se orientan hacia las tecnologías de la información, el cuidado de los datos se ha hecho cada vez más importante, tanto así que la información en la actualidad es considerada un activo más en la organización, por ésta razón, el presente documento expresa la importancia de mantener segura la información, de qué forma se debe generar una cultura de seguridad al interior de la empresa y como esa cultura debe ser manejada y trasplantada dentro de los trabajadores de una organización.

A lo largo del documento se presentan elementos que fundamentan la importancia de consolidar la seguridad de la información empresarial además de generar una herramienta para la concientización del recurso humano de una organización en pro de la conservación de la información en ambientes seguros.

Palabras Clave— Cultura de la seguridad, información, privacidad, seguridad

I. INTRODUCCIÓN

La seguridad informática es uno de los elementos que sugiere mayor preocupación en las empresas que han entendido el valor de la información, en los datos, se encuentran contenidos los antecedentes de la empresa, sus debilidades, fortalezas, entre otros aspectos que representan las características de la organización y prácticamente sintetizan la estructura de la empresa.

En la actualidad, se considera que la información es de tanta importancia para la empresa moderna que simplemente si se gestiona de forma eficaz puede llegar a beneficiar el desarrollo de la empresa, la información sugiere tanta importancia para una empresa que puede ser utilizada de forma simultánea, no se gasta con el uso y los fragmentos de la misma pueden ser combinados entre sí para generar más información. [1]

La información llega a la empresa y a sus empleados de diferentes formas, puede llegar por fenómenos internos o por fenómenos externos, sin embargo la capacidad para asimilar dicha información por parte de los empleados no se consigue de repente y por el contrario, debe ser construida por la empresa como parte de la cultura organizacional.

Esa cultura organizacional basada en la importancia de la seguridad informática se fomenta a través de la motivación que se da a los usuarios ante la importancia de conservar la información empresarial, ésta, cada vez suele ser más vulnerable puesto que los atacantes de la información cada vez amenazan con técnicas diversas que sencillamente pueden llegar a violar las características del usuario final. [2]

A partir de la relevancia que tiene la información organizacional y la importancia de que los empleados de una empresa sean concientizados del manejo seguro de la información, se desarrolló el presente artículo, en donde se recolectaron cifras e investigaciones previas referentes a la importancia de la seguridad, las formas en cuales la seguridad organizacional se puede ver afectada y las formas de contrarrestar la violación a la información desde la cultura organizacional y los colaboradores de una empresa.

II. METODOLOGÍA

La descripción de la seguridad en la información nace desde el mismo origen de la información en las empresas, cuando se empezaron a establecer los datos a través de herramientas tecnológicas, sin embargo, los antecedentes registrados de la protección a la información datan de hechos no recientes.

Las primeras muestras de protección a la información, se describen desde la Segunda Guerra Mundial, con la "Máquina enigma" en la cual se destacaba la protección a los archivos nacionales, siendo esta la primera evidencia de protección a la información. [3]

La preocupación a la seguridad de la información, trasladada a la tecnología data de 1980 cuando James P. Anderson, redactó un documento titulado "Computer Security Threat Monitoring and Surveillance" en donde se desarrollan los primeros conceptos de amenazas informáticas. [3]

Dentro de los conceptos más relevantes de la seguridad informática, se destacan la vulnerabilidad y el ataque, los cuales deben considerarse para las prácticas de protección a la información en redes y en herramientas tecnológicas, las medidas de defensa pueden darse desde el hecho de evitar amenazas en donde surgen términos como virus y antivirus que hasta la actualidad se han convertido en términos cotidianos, debido a que las tendencias de la vida moderna han generado una obligatoriedad al uso de las herramientas informáticas como consecuencia de los cambios en el almacenamiento de la información y en la operatividad de las empresas. [3]

Las amenazas a la información generalmente son humanas y surgen como consecuencia de la necesidad inescrupulosa de afectar o acceder a la información de terceros, los agentes comúnmente conocidos que afectan la seguridad de la información son los hackers, quienes tienen una intención primaria de rastrear la información dejada por un usuario, para luego ingresar de forma inadvertida a bases y en ocasiones su intención es más grave ya que buscan vender la información obtenida al mejor postor. [4]

De acuerdo con estos antecedentes, se puede destacar la seguridad informática para las empresas, éste término, consiste principalmente en la implantación de medidas técnicas en donde se busca generar confidencialidad, disponibilidad de la información, responsabilidad de la información que se publica y se almacena y responsabilidad dada en los individuos que manipulan dicha información.

La seguridad informática, es un tema clave para las organizaciones modernas, puesto que la gran mayoría de ellas documentan sus actividades tanto comerciales como financieras en herramientas informáticas en donde se da el acceso a ella a diferentes tipos de usuarios, los cuales deben velar por la seguridad y defensa de la información, además de las estrategias de protección que debe

implementar la empresa para impedir que existan posibles violaciones de la información. [4]

III. DISCUSIONES Y RESULTADOS

Es importante describir inicialmente que la seguridad no solamente se da desde el interior sino también desde el exterior, la información exterior se provee a partir de los usuarios que van a manipular la información y la seguridad interior se provee a partir de las barreras que protección que se generan dentro del software o programa de manejo de información. [5]

El internet, permite la filtración de muchas formas de violación de la información, sin embargo muchas de las fallas son de carácter humano, todo como consecuencia de una escasa cultura de seguridad de la información. La concientización de los empleados en una empresa podrá sugerir una buena forma de proteger la información y generar seguridad desde el interior, las fallas humanas pueden llegar a proporcionar la mejor oportunidad para los atacantes de filtrarse en la organización. [2]

Los primeros antecedentes de ataques a la seguridad informática, se atribuyen al expresidente de Estados Unidos Ronald Reagan, quien habría vendido a la URSS algunos computadores y equipos que contenían dentro de sí una serie de códigos fuente de software que permitían entonces la violación a la información que se contuviera en dichos equipos. [3]

En este contexto, el desconocimiento del recurso humano con respecto al manejo de la información y su importancia pusieron en evidencia datos claves que pudieron haber modificado incluso las más importantes estrategias.

Así mismo, las empresas pueden estar exponiendo su información estratégica a la competencia y luego encontrarse con que la competencia se ha adelantado a las decisiones de la organización, con el fin de evitar que este tipo de problemas sorprendan a la empresa, se han desarrollado formas de concientizar a los empleados de la organización con respecto al cuidado de la información.

Esta concientización solamente se puede generar a partir de la construcción de una cultura de seguridad de la información en donde se distinguen tres factores influyentes que son Cumplimiento, Apropiación y Concienciación.

La apropiación es una acción que permite a los empleados hacerse responsables de sus acciones y así mismo conscientes de su papel en la protección de la información, la empresa, debe lograr en el empleado ese nivel de interiorización para adaptar sus creencias personales a sus creencias corporativas en donde se entienda que la información de la empresa es tanto o más valiosa que su propia información. [2]

Fuente: IT-Insecurity [2]

El empleado debe ser consciente de la importancia de la información empresarial como foco para la generación de estrategias.

El proceso de la concienciación busca que los individuos se hagan conscientes de los riesgos y amenazas que pueden surgir en torno a la información empresarial, así mismo, se deben hacer responsables de reportar todos aquellos problemas de desviación de información que evidencien como falla en la seguridad. [2]

El último elemento a considerar en el proceso de culturización a los empleados en torno a la seguridad informática es el cumplimiento, este elemento se relaciona con la adherencia del empleado a las políticas, procedimientos y prácticas

de seguridad de la información existentes. Cabe destacar que todas las formas de protección a la seguridad informática son responsabilidad de todos los empleados de la organización quienes deben servir de veedores y auditores del manejo de que se le da la información, de las características de la persona que accede a ella y los permisos de usuarios que se otorgan a cada empleado.

Es igual responsabilidad de la empresa, puesto que debe saber otorgar responsabilidades, además de garantizar la protección interna desde los equipos hasta el software mismo.

IV. CONCLUSIONES

El éxito de la seguridad informática, se puede alcanzar a través de la conjugación eficiente de tres elementos que son Gobierno Corporativo, Cultura Organizacional y Seguridad de la Información.

Estas relaciones generan un producto entre sí que a su vez integran una serie de decisiones de carácter estratégico que fundamentan la seguridad informática y su relación con las responsabilidades de empleados y administrativos de la empresa.

Fuente: Thompson (2007) [6]

La relación A, exige el hecho de que una organización reconozca y declare a la información como un activo de la empresa en donde se responsabilice a la administración de la empresa como responsable de su información y el cuidado de la misma. [6]

La relación B, demanda que las acciones, comportamientos empresariales y creencias se encuentren sujetos de forma positiva a los empleados de la empresa en donde la empresa busque cultivar comportamientos saludables con respecto al tratamiento de la información los cuales deben estar adheridos a las políticas empresariales. [6]

La relación C, se define entorno a los comportamientos que son aceptables y no aceptables en donde la empresa declara que su misión y visión da cumplimiento a la información que se genera y se expone al público así como la que se mantiene en privado.

Por último, la relación D, determina la relación importante entre la cultura de la organización y las acciones de los empleados dentro de la misma

REFERENCIAS

[1] Lic. Arribas, U. A., 2000. Comunicación en la empresa. La importancia de la información interna en la empresa. Revista Latina de Comunicación Social, Volumen 27.

[2] IT-insecurity, 2014. Cultura organizacional de seguridad de la información. Factores clave, relaciones relevantes e impactos organizacionales. [En línea] Disponible en: http://insecurityit.blogspot.com/2014/01/cultura-organizacional-de-seguridad-de.html [Último acceso: 06 Agosto 2014].

[3] PortalTic, 2014. La seguridad de la información en la era de la informática. [En línea] Disponible en: http://www.europapress.es/portaltic/sector/noticia-seguridad-informacion-era-informatica-20101130080003.html [Último acceso: 06 Agosto 2014].

[4] Segu-info, 2009. Amenazas Humanas - Historia Hacker. [En línea] Disponible en: http://www.segu-info.com.ar/amenazashumanas/historia-hacker.htm [Último acceso: 06 Agosto 2014].

[5] Montenegro, L., 2012. Microsoft. [En línea] Disponible en: http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/ [Último acceso: 06 Agosto 2014].

[6] Thompson, K., 2007. Model for information security shared tacit espoused values. Unpublished Doctoral Thesis. [En línea] Disponible en: http://dspace.nmmu.ac.za:8080/jspui/handle/10948/717 [Último acceso: 06 Agosto 2014].