Artículo **Revista de Tecnologías de la Información y Comunicaciones**
Septiembre, 2018 Vol.2 No.5 11-15

Importancia de la capacitación del personal a través de una cultura de seguridad informática

Importance of staff training through a culture of computer security

VILLAGRAN-VIZCARRA, Dafnis Cain†*, RAMÍREZ-OCHOA, Dynhora Danheyda, BARBA-MARTÍNEZ, Cristina y BARROSO-BARAJAS, Alfonso José

Universidad Tecnológica de Chihuahua, Ave. Montes Americanos 9501, Sector 35, CP. 31216, Chihuahua, Chih

ID 1er Autor: *Dafnis Cain, Villagran-Vizcarra* / **ORC ID:** 0000-0001-5611-9834, **Researcher ID Thomson**: X-3134-2018, **CVU CONACYT ID**: 953360

ID 1er Coautor: *Dynhora Danheyda, Ramírez-Ochoa* / **ORC ID:** 0000-0002-1326-908X, **Researcher ID Thomson**: X-3130-2018, **CVU CONACYT ID**: 521748

ID 2do Coautor: *Cristina, Barba-Martínez* / **ORC ID:** 0000-0001-5966-9428, **Researcher ID Thomson**: X-3164 -201

ID 3er Coautor: *Alfonso José, Barroso-Barajas* / **ORC ID:** 0000-0002-5353-5987, **Researcher ID Thomson**: X-3133-2018, **CVU CONACYT ID**: 521749

Recibido 17 de Julio, 2018; Aceptado 08 de Septiembre, 2018

Resumen

La información que manejan todas las empresas se ha vuelto un activo muy importante, debiendo ser salvaguardado y protegido por diferentes herramientas de seguridad. En la actualidad el tema de seguridad se ha vuelto muy importante y se puede encontrar una gran cantidad de información acerca del tema, sirviendo a las empresas para evitar algunas de las amenazas y vulnerabilidades, pero la falta de una cultura de seguridad informática con todo su personal llega a generar la infiltración de información o fallas en la seguridad exponiendo la información a intrusos informáticos. El proyecto se basa en la determinación de los riesgos y vulnerabilidades, a través de un análisis de fallas de seguridad informática, que enfrentan diversas empresas del sector productivo brindando una propuesta de solución. En donde los resultados que se presentan radican en el contenido de la capacitación que se da al personal para reducir los riesgos de seguridad y el mal manejo de los datos.

Seguridad Informática, Cultura Informática, Riesgos, Amenazas, Vulnerabilidades

Abstract

The information handled by all companies has become a very important asset, which must be safeguarded and protected by different security tools. Currently, the security issue has become very important and a lot of information can be found about this topic. This has helped the companies to avoid some of the threats and vulnerabilities, however the personnel´s lack of a culture about computer security can generate information infiltration or security failures exposing the information to computer intruders. The project is based on the determination of risks and vulnerabilities through an analysis of computer security failures faced by various companies in the productive sector, so a solution proposal is provided. The results presented lie in the content of the training given to the company´s staff in order to reduce security risks and data mishandling.

Information Security, Computer Culture, Risks, Threats, Vulnerabilities

Citación: VILLAGRAN-VIZCARRA, Dafnis Cain, RAMÍREZ-OCHOA, Dynhora Danheyda, BARBA-MARTÍNEZ, Cristina y BARROSO-BARAJAS, Alfonso José. Importancia de la capacitación del personal a través de una cultura de seguridad informática Revista de Tecnologías de la Información y Comunicaciones. 2018. 2-5: 11-15

* Correspondencia del Autor (Correo electrónico: dvillagran@utch.edu.mx)
† Investigador contribuyendo como primer autor.

Introducción

El siguiente artículo expone la existente problemática dentro de instituciones y empresas del sector productivo de la ciudad de Chihuahua, Chihuahua, México, donde el manejo de las Tecnologías de Información y Comunicación (TIC) es de gran relevancia para las compañías. Indicando el contenido que se debe brindar al personal para un programa de capacitación permanente, para apoyar al desarrollo de una cultura de seguridad informática que impacte en la mejora de los procesos de seguridad dentro la empresa y al mismo tiempo reducir las vulnerabilidades en cuanto al manejo de la información.

La investigación se divide en las etapas de: reconocimiento de los riesgos, identificación de los riesgos, determinación del contenido de la capacitación y acciones que deben llevarse a cabo, teniendo como principal objetivo el análisis en eventos críticos y su solución a través de la cultura de seguridad informática que ayudará a la sensibilización del personal de las empresas para mejorar la seguridad de la información.

Justificación

La presencia en Internet es indispensable para cualquier empresa en los tiempos actuales, ya que es una manera de mostrar la información de la organización a sus clientes potenciales y con esto incrementar la capacidad de expansión de la empresa. Debido al alto nivel de exposición y uso de las herramientas TIC, los activos más importantes de la empresa están propensos a vulnerabilidades y amenazas, tanto internas como externas.

Por esta razón es indispensable llevar a cabo un análisis sistemático de los riesgos que tiene el uso de dichas tecnologías y preparar al personal para poder afrontarlos con éxito.

En estas situaciones es conveniente realizar análisis basados en el estándar ISO/IEC 27002 para identificar las vulnerabilidades y clasificarlas de acuerdo con su prioridad, para estar en condiciones de resolver problemas y tomar acciones preventivas y correctivas en materia de seguridad informática dentro de la empresa.

Problema

– Los grandes volúmenes de información y el incremento de las TIC dentro de la forma de vida de las personas conllevan a que ésta se encuentre disponible y actualizada en tiempo real, teniendo un alto grado de inseguridad.
– El mal manejo o descuido de las TIC por parte de los empleados de manera consciente o inconsciente perjudican en la infiltración de la información.

Hipótesis

Un alto grado de seguridad en el manejo de la información dentro del personal de una empresa, se puede lograr mediante la sensibilización del manejo adecuado de la información de manera permanente, desarrollando una cultura de la seguridad informática.

Objetivos

Reducir los riesgos de inseguridad y el mal manejo de los datos, a través del desarrollo de una cultura informática para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de las empresas mediante una capacitación permanente al personal.

Reducir las amenazas de seguridad mediante el análisis de las vulnerabilidades en el manejo de la información en los sistemas que utilizan dentro de las empresas.

Marco Teórico

Para tener un sistema seguro se debe analizar la posibilidad de que una amenaza se materialice (vulnerabilidad) contra los activos con los que cuenta la empresa —datos, software, hardware, redes, soportes, instalaciones, personal y servicios— tomando en cuenta los factores atacantes que altera, daña o tiene acceso a la información de manera ilegal (conocido como amenazas) y el impacto que se tendrá de manera cuantitativa o cualitativa (Aguilera, 2010).

Los ataques a los activos de las empresas por lo general implican graves consecuencias y daños irreparables, se estima que en México 1.5 millones de personas son afectadas por ciberataques a diario, además se generan pérdidas de hasta 111,000 millones de dolares.

ISSN 2531-2200

En donde el 49% de los responsables de ataques ciberneticos son empleados de menor rango, 37% son realizados por excolaboradores y el 34% por proveedores. Y solo el 50% de las compañias cuenta con personal capaz de enfrentar dicha problemática (Forbes, 2018) .

Debido a la velocidad con que evoluciona la tecnología el estándar ISO/IEC 27002 propone más de 130 controles relacionados con aplicaciones, dispositivos tecnológicos, recursos humanos y cuestiones organizativas para implementar tomando en cuenta la tecnología, personas y procedimientos (Montesino, Baluja & Porvén, 2013).

Según la investigación realizada por Ramírez, Barroso, Siqueiros y Villagrán (2017) se observa que los ataques que experimenta una empresa pueden ser accidentales o de manera deliberada contra algún activo de la empresa, los cuales agreden de manera directa o indirecta. Es decir, causan algún riesgo a un activo específico o son el medio para llegar a otro lugar al cual se quiere atacar.

Y que estos se pueden reducir implementando una capacitación permanente en materia de seguridad informática a todo el personal de la empresa, siendo un factor clave para mantener la seguridad, por lo que debe de tomarse en cuenta no solo la formación, sino la educación y concientización del personal para desarrollar una cultura informática, lo cual se ve en el estándar ISO/IEC 27002.

Metodología de investigación

El proyecto está basado en la investigación comprensiva, ya que se explican las vulnerabilidades y amenazas que puedan ocurrir, predicen el riesgo e impacto que generará y proponen una solución para elevar el grado de seguridad informática.

Utilizando los tipos de investigación:

– Hipotética deductiva: para demostrar que una cultura informática puede reducir los riesgos de seguridad en una empresa.
– Descriptiva: ya que se describe los procesos que se llevan a cabo y aquellos que son planeados en el objetivo de estudio.

Análisis de las vulnerabilidades y amenazas de seguridad informática

La seguridad informática no es algo que se alcanza y se sostiene en un determinado tiempo, o que se logra al 100%, debido a que éste se obtiene mediante la implementación de controles de seguridad que incluyen activos dinámicos (políticas, procedimientos, estructuras y equipamiento con el que cuenta las empresas).

Es por ello, que la seguridad informática es un proceso continuo que debe de utilizar un modelo PDCA (*Plan-Planificar, Do-hacer, Check-verificar, ACT-Actuar*) e implementar las siete acciones que marcan los niveles de control de seguridad del ISO/IEC 27002 (*establecer, implementar, operar, monitorizar, revisar, mantener y mejorar*) para aumentar el grado de seguridad.

Identificación de riesgos

Para poder identificar los riesgos que tiene una empresa debe de aplicar un proceso de análisis tomando en cuenta los siguientes pasos mencionados por Montesino et al. (2013):

1. Hacer inventario y valoración de los activos.
2. Identificación y gestión de los usuarios.
3. Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.
4. Identificar y evaluar las medidas de seguridad existentes.
5. Identificar y valorar las vulnerabilidades de los activos a las amenazas que le afectan.
6. Identificar los objetivos de seguridad de la organización.
7. Determinar sistemas de medición de riesgos.
8. Determinar el impacto que produciría un ataque.
9. Identificar y seleccionar las medidas de protección.

Los mecanismos y herramientas de seguridad se clasifican de acuerdo con lo que desempeñan: preventivos, detectores o correctores. Éstos pueden ser para: el control de acceso, antivirus, cortafuego, firmas digitales, certificados digitales, protección de red mediante claves encriptadas, respaldo de datos, dispositivos físicos, etc.

ISSN 2531-2200

Determinación de riesgos

Para proteger la información es necesario tomar en cuenta los niveles: ubicación física, hardware y componentes de la red, el sistema operativo, todo el software instalado, la conexión a internet y la información que se maneja. De acuerdo con eso se tienen mecanismos y servicios de seguridad adecuados a cada nivel.

A través del análisis de diversas instituciones y empresas del sector productivo se comparan algunas acciones importantes en cuestiones de seguridad informática. Las principales se muestran las en la Tabla 1, donde las empresas consideradas se pueden apreciar con la siguiente numeración: Universidad Tecnológica de Chihuahua (1), Profesionales en comunicaciones e informática (2), Funerales Miranda (3), Instituto Mexicano del seguro social (4), Escuela secundaria técnica #62(5).

Acciones y estrategias	Empresas				
	1	2	3	4	5
Actualizar SW-HW	x	x		x	
Copias de seguridad distribuidas	x				
Servicios de alta disponibilidad		x			
Cultura informática					
Revisión periódica de procesos de seguridad	x	x			
Personal o área en TI	x	x	x	x	x
Capacitación en ciberseguridad	Básica	Básica			

Tabla 1 Acciones y estrategias observadas en empresa del sector productivo
Fuente: Análisis de investigación, propia

Derivado del análisis de las amenazas y vulnerabilidad de las empresas, se determina lo siguiente:

– La mayoría cuenta con personal o alguna área dedicada a las tecnologías de la información (TI).
– El 60% de las empresas basan su seguridad en infraestructura de hardware (HW) y software (SW).
– Solo el 25% de las empresas brinda capacitación en ciberseguridad, pero ésta es básica, por lo que el personal de TI está limitado para poder resolver ataques, violaciones o infiltraciones de intrusos.

Resultados

Para la implementación y desarrollo de las estrategias que se recomiendan, las empresas deben de apoyarse de las sugerencias de expertos en el área de seguridad y los encargados dentro de la empresa de TI, para poder implementar estrategias y acciones, con el siguiente contenido:

1. Dar capacitación al todo el personal de la empresa al ingresar sobre los temas:

– Manejo de la información, contenidos y documentos personales a compartir en internet, para evitar infiltraciones o manejos inadecuados de información.
– Cuidado de la información de los dispositivos móviles.
– Políticas de acceso para sitios web, para sensibilizar las restricciones que indica la empresa.
– Identificación de sitios e hipervínculos seguros.
– Reconocer archivos no maliciosos en correos electrónicos y protección de software.
– Determinación del software que se puede instalar y cómo instalarlo en los equipos.

2. Las áreas de TI o personal encargado deberán trabajar con las políticas de seguridad contemplando los puntos:

– Plan de actualización del hardware y software.
– Realizar un plan de respaldo de información.
– Contratar servicios de alta disponibilidad.
– Tener una revisión periódica de los procesos de seguridad.

3. Capacitación en temas de ciberseguridad a los empleados encargados de tecnologías de la información y actualizaciones para todo el personal.

La implementación de determinadas medidas de seguridad puede resultar incómoda para muchos usuarios del sistema y, por ello, resulta fundamental contemplar la adecuada formación, concientización y sensibilización de los usuarios para que estas medidas se puedan implantar de forma efectiva.

ISSN 2531-2200

Conclusiones

Con la investigación se concluye que es esencial la capacitación en diferentes tiempos y grados de profundidad para poder aumentar el nivel de seguridad dentro de toda organización. Contando con un programa de capacitación permanente para todo el personal en el que se eduque, forme y tomen conciencia de la seguridad que deben tener de manera personal, profesional y organizacional; ya que la clave del éxito no depende solamente del equipamiento y configuración del Hardware y Software para proteger los activos, si no de tener una cultura informática en el personal, y de esa manera elevar el grado de seguridad informática de la empresa para sus activos.

Referencias

Aguilera, L. P. (2010). *Seguridad informática*. España: Editex S.A.

Forbes. (2018). Mexicanos reciben 1.5 millones de ataques cibernéticos al día. Recuperado de https://www.forbes.com.mx/mexicanos-reciben-1-5-millones-de-ataques-ciberneticos-al-dia/

Montesino, P. R., Baluja, G.W. & Porvén, R. J. (2013). Ingeniería electrónica, automática y comunicaciones. *Gestión automatizada de controles de seguridad informática, 34*(1), 40-58. Recuperado de http://scielo.sld.cu/scielo. php?pid =S181 5 59282013000100004&script =sci_arttext&tlng=pt

Ramírez, O. D., Barroso, B. A., Siqueiros, G. M. & Villagrán, V. D (2017). The computer security culture reduces the risk of information loss and leakage. *RINOE Journal-Schools of economic thought and methology, 1*(1), 29-35.

ISSN 2531-2200