Revista de la Escuela de Estudios de Postgrado, Vol. 7 No. 1, año 2016.
ISSN 2518-4725.

PROYECTO DE EMPRENDIMIENTO EMPRESARIAL EN EL DISEÑO DE SOLUCIONES A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA TEORÍA GENERAL DE DISUASIÓN

Alicia Eugenia Ruano Aguilar
Mtro. en Tecnologías de la Información y la Comunicación
aliciara1954@gmail.com

Everest Darwin Medinilla
Asesor
Mtro. en Administración de Negocios
emedin@gmail.com

Resumen

Aunque las empresas u organizaciones de cualquier segmento o ámbito ya cuentan con tecnologías de seguridad como por ejemplo: software antivirus, dispositivos de red y firewalls, estas tecnologías no satisfacen por completo la seguridad de la información.

Con base a la problemática planteada, se procedió a identificar los riesgos de la seguridad de la información en diferentes organizaciones por medio de una encuesta elaborada con base en los constructos que componen la Teoría General de Disuasión.

El objetivo general del trabajo de graduación es el emprendimiento empresarial en el diseño de soluciones a riesgos de seguridad de la información, dichas soluciones pueden mencionarse: la concientización y capacitación al empleado, uso de medios disuasivos, elaboración de la política de seguridad y su divulgación, uso de tecnología informática y definición de estrategias de mejora continua.

El impacto de la implementación de estas soluciones en las organizaciones, garantiza la protección de uno de sus principales activos que es la información.

Palabras clave

Seguridad, información, teoría, disuasión, emprendimiento.

Abstract

Although businesses or organizations of any segment or area already have security technologies such as: antivirus software, network devices and firewalls, these technologies do not fully meet safety.

Based on the issues raised, we proceeded to identify the risks of information security in different organizations through a survey conducted based on the constructs that make up the General Theory of Deterrence.

The overall objective of graduate work is entrepreneurship in design solutions to security risks of information based on the General Theory of Deterrence (GDT), this was achieved through the creation of a business plan.

The impact or key activity was taken into account in drawing up the plan, was to offer businesses security policy development and awareness of staff on issues of information security as one of the main solutions.

Keywords

Security, information, theory, deterrence, entrepreneurship.

Desarrollo del estudio

El acceso no autorizado a una red informática o a equipos que en ella se encuentren puede ocasionar graves problemas, algunas de las posibles consecuencias de una intrusión son la pérdida de datos, robo de información sensible o confidencial, divulgación de información sobre clientes, ingeniería social (técnica psicológica para persuadir a un individuo), intercambio de contraseñas por correo electrónico, entre otros.

En este trabajo de investigación se llevó a cabo el análisis cualitativo de una serie de datos recolectados, para identificar los principales riesgos de la seguridad de la información.

Posteriormente, se desarrolló un plan de negocio para el emprendimiento de una empresa dedicada al diseño de soluciones a riesgos de seguridad de la información, dicho plan describe los segmentos de mercado, actividades clave, recursos clave, costos y canales a ser tomados como actividades del emprendimiento.

Detmar, Straub y Richard en 1998, analizan el concepto de Teoría General de Disuasión aplicado a riesgos de seguridad de la información. Aseguran con base a resultados, que ningún sistema puede ser absolutamente seguro, por lo tanto, la inadecuada seguridad en muchas organizaciones es una situación que puede y debe remediarse aplicando teorías (término en inglés theorybased) que sirven como herramientas para la planificación de la seguridad (Straub &Welke, 1998).

Schuessler (2009), indica que la disuasión se define como "la inhibición de la conducta criminal por el miedo, sobre todo de la pena", en otras palabras, las actividades de disuasión proveen desincentivos para los posibles abusadores de ordenador. Los ejemplos de los esfuerzos de disuasión incluyen "las políticas administrativas, capacitación de los empleados, y las funciones de seguridad visibles" (Schuessler, 2009).

La Teoría de General de Disuasión se fundamenta en cuatro variables: la disuasión, prevención, detección y corrección.

La prevención se define como un estorbo o un obstáculo. Estos pueden incluir obstáculos físicos tales como guardias, puertas cerradas, y así sucesivamente y/o herramientas de software tales como dispositivos de autenticación y firewalls.

La detección se define como el acto o proceso de descubrimiento. Lo que se refiere a los sistemas de información, es el proceso de tratar de descubrir las violaciones de seguridad dentro de una organización mediante el examen de los registros del sistema, informes de monitoreo de actividades sospechosas, y así sucesivamente.

Remedio o corrección se define como un orden jurídico de prevenir o reparar un daño o hacer cumplir un derecho, ya sea por medio de sanciones internas tales como reprimendas o terminación, o externamente por la vía legal o sistemas de regulación.

Lo anterior se muestra en la Figura 1.

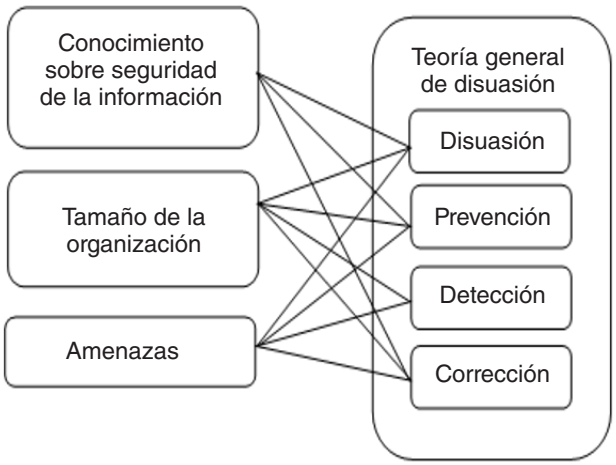

Figura 1. Teoría General de Disuasión.
Fuente: General Deterrence Theory: Assesin Information Systems Security Effectiveness in Large versus Smal Business por Joseph H. Schuessler, 2009.

Resultados obtenidos

Según Mahía Casado (2004), el análisis factorial es una técnica de reducción de datos, que sirve para encontrar grupos homogéneos a partir de un conjunto numeroso de variables. Para este análisis

se toman como variables latentes las diferentes preguntas planteadas en una encuesta que se elaboró tomando como base los siguientes constructos:

Conocimiento sobre seguridad de la información	=	CS
Tamaño de la organización	=	TO
Amenazas	=	AM
Disuasión	=	DS
Prevención	=	PV
Corrección	=	CR

Al obtener los datos iniciales del análisis factorial, se obtuvo una matriz de factores no rotada, ésta fue sometida posteriormente a un procedimiento de rotación.

La Tabla I muestra los resultados de la rotación realizada, se resaltan los resultados de los factores con los valores más altos.

Tabla I. *Matriz de factores rotados.*

	Factor 1	Factor 2	Factor 3	Factor 4
CS1	0.145	0.172	0.515	
CS2		0.274	0.716	
PV1		0.709	0.133	
PV2	0.194	0.227	0.534	
PV3	0.581	0.479		
PV4	0.343	0.199	0.181	0.242
PV5		0.453		0.839
CR1	-0.205	0.689	0.204	
CR2		0.637	0.177	0.173
CR3	0.558	0.568	0.266	0.159
DS1	0.447	0.248		0.116
DS2		-0.131		0.501
AM1	0.881			-0.124
AM2	0.620		0.248	
AM3	0.847	-0.190	0.109	

Fuente: elaboración propia.

Con base a resultados obtenidos, se procede a renombrar los factores. Los nombres se derivan de la agrupación de combinaciones lineales con valores propios de mayor peso.

Factores renombrados: Factor 1 se denomina Riesgos, ya que los valores propios con mayor peso únicamente se ven reflejadas en las variables de Amenazas, el Factor 2 se denomina Integridad de la Información, los valores propios con mayor peso se relacionan con la prevención y corrección, el Factor 3 se denomina Confidencialidad, ya que los valores con mayor peso se ubicaron en las variables de conocimiento sobre seguridad de la información; por último, al Factor 4 Disponibilidad de la Información ya que los valores con mayor pesos se ubicó en la variable Prevención.

La Figura 2 representa gráficamente cómo están relacionados los constructos que conforman la teoría con cada enunciado de la encuesta realizada que a su vez fue clasificada, según el aspecto a evaluar.

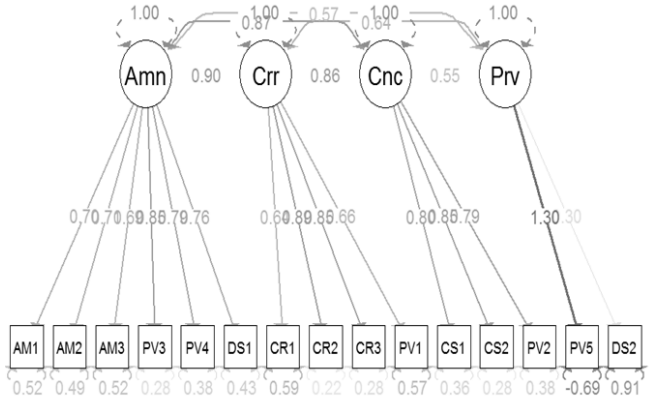

Figura 2. Representación gráfica del modelo.

Fuente: elaboración propia.

Discusión de resultados

Luego de analizar el diagrama del modelo obtenido en el análisis confirmatorio, se puede observar que la prevención se relaciona también con las correcciones, lo que corresponde a garantizar la integridad de la información, sin duda, son dos aspectos que van de la mano.

Las organizaciones tienen que definir cómo actuarán si se llega a materializar algún tipo de riesgo y qué medidas de prevención están tomando en cuenta, así mismo, una de las prevenciones puede ser el factor disuasión, que se refiere al efecto que estén causando sobre los usuarios de sistemas o empleados.

En una de las preguntas de respuesta abierta para la primera encuesta entregada a 50 personas, coincidieron que una de las principales razones por las que existen riesgos en la seguridad es porque los empleados no tienen conocimiento del tema y otra razón es que las organizaciones no cuentan con políticas de seguridad establecidas, por lo tanto no se puede garantizar la confidencialidad.

Siguiendo la línea de investigación y basado en los antecedente presentados, el argumento base de este trabajo, se enfoca en que las acciones de seguridad de la información que se apliquen puede disuadir a potenciales abusadores informáticos de cometer actos que violen implícita o explícitamente la política de la organización.

La aplicación específica de la teoría se basa en la relación entre las actividades de los altos mandos y los posibles abusadores, en primer lugar deberían ser los directivos la clave para disuadir con éxito y garantizar la prevención y detección del abuso, así como contar con los recursos que permiten castigar a los delincuentes.

Una cierta porción de potencial de abuso es disipado mediante técnicas de disuasión, como las políticas y directrices para el uso adecuado del sistema de información y recordatorios a los usuarios a cambiar sus contraseñas.

Programas de concientización de seguridad son una forma de contramedida disuasiva que no se debe obviar, es decir, la educación a los usuarios, así como a sus superiores acerca de la seguridad, produce grandes beneficios.

Estas sesiones educacionales transmiten conocimiento sobre los riesgos en la organización, como por ejemplo: dar a conocer las políticas y las sanciones por violaciones, revelar las amenazas a los sistemas locales y su vulnerabilidad a los ataques y enseñar al usuario cómo debe actuar ante ataques, para lograr el objetivo que se persigue, que es la seguridad.

Para este trabajo especial de graduación se brinda la propuesta de diseño de solución a las problemáticas de los riesgos de seguridad de la información identificados en la evaluación y análisis realizado en el punto anterior. Los aspectos a destacar de la solución son los siguientes:

- Conocimiento sobre seguridad de la información
- Política de seguridad de la información

La solución está basada bajo las premisas de la norma internacional ISO/IEC 27001, tecnología de la Información, técnicas de seguridad y código para la práctica de la gestión de la seguridad de la información.

Conclusiones

1. Se concluye que los dos principales riesgos en seguridad de la información son: la falta de conocimiento en seguridad de la información por parte de los empleados y la inexistencia de una política de protección de información que sea conocida por los mismos.
2. Entre las medidas que pueden implementarse para mitigar los riesgos de la seguridad de la información están las siguientes: el uso de medios disuasivos, diagnósticos periódicos, establecer una política de seguridad de la información, capacitaciones al personal, el uso de la seguridad informática y gestionar la seguridad de la información de forma permanente.
3. El uso de medios disuasivos, como lo indica La Teoría General de Disuasión, permite que los individuos se abstengan de cometer actos delictivos que violen la seguridad de la información de una organización.

Recomendaciones

1. A organizaciones y público en general, la utilización de la Teoría de Disuasión General puede aplicarse no sólo para la identificación y solución de riesgos en seguridad de la información, sino que también puede ser aplicada a otros temas, donde se requieran métodos disuasivos para llevar el control de determinado evento, proceso o problema.

2. A organizaciones en general, la utilización de herramientas o medios disuasivos dentro de la empresa como prevención.
3. A cualquier persona que desee emprender el uso de la herramienta de lienzo de negocio, ya que facilita comprender y ordenar las ideas para elaborar de una manera sencilla un plan de negocio.
4. A empresas que comienzan operaciones, establecer canales informativos que proporcionen a los emprendedores los conocimientos u orientaciones necesarias, para incorporar la seguridad de la información y la continuidad del negocio como áreas de la estrategia empresarial.
5. A estudiantes de Maestría en Tecnologías de la Información y Comunicación, el uso del análisis estadístico en los casos que el trabajo de investigación requiera un estudio de campo, facilita la interpretación de los datos para fundamentar soluciones, conclusiones o argumentos que el trabajo de investigación presente.

Referencias bibliográficas

Baltazar Gález, J. M., & Compuzano Ramírez, J. C. (2011). D*iseño e implementación de un esquema de seguridad perimetral para redes de datos.* México: Universidad Nacional Autónoma de México.

Mahía Casado, R. (2014). *Análisis Factorial.* Recuperado de http://www.uam.es/personal_pdi/economicas/eva/pdf/factorial.pdf

Montenegro, L. (2014). *Seguridad de la información: más que una actitud, un estilo de vida.* Recuperado de: http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

Schuessler, J. H. (2009). *General deterrence theory: assesin information systems security effectiveness in large versus small business.* Recuperado de: http://nsl.cse.unt.edu/~dantu/cae/attachments/JosepthSchuesslerDissertation.pdf

Straub, D., & Welke, R. (1998). *Coping with systems risk: Security Planning Models for Management Decision Making.* Recuperado de: http://paul-hadrien.info/backup/LSE/IS%20490/utile/Straub%20G%20DT.pdf