INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CENTRO DE INVESTIGACIONES ECONÓMICAS, ADMINISTRATIVAS Y SOCIALES

Gestión de la seguridad de la información en la empresa

TESIS

QUE PARA OBTENER EL GRADO DE:
MAESTRO EN POLÍTICA Y GESTIÓN DEL CAMBIO TECNOLÓGICO
PRESENTA:

OSCAR RAÚL ORTEGA PACHECO

DIRECTORES

RAÚL VÁZQUEZ LÓPEZ
MIJAEL ALTAMIRANO SANTIAGO

MÉXICO, D.F. NOVIEMBRE, 2010

SIP-14-BIS

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de MÉXICO, D.F. siendo las 17:30 horas del día 30 del mes de NOVIEMBRE del 2010 se reunieron los miembros de la Comisión Revisora de Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de CIECAS para examinar la tesis titulada:

"GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA"

Presentada por el alumno:

ORTEGA	PACHECO	OSCAR RAÚL
Apellido paterno	Apellido materno	Nombre(s)

Con registro: B 0 8 1 9 7 8

aspirante de:

MAESTRÍA EN POLÍTICA Y GESTIÓN DEL CAMBIO TECNOLÓGICO

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Directores de tesis

DR. RAÚL VÁZQUEZ LÓPEZ

DR. MIGUEL ALTAMIRANO SANTIAGO

DRA. HORTENSIA GÓMEZ VIQUEZ

DR. RUBÉN OLIVER ESPINOZA

DR. HUMBERTO MERRITT TAPIA

DR. [illegible] JIMÉNEZ DOMÍNGUEZ

PRESIDENTE DEL COLEGIO DE PROFESORES

DR. ZACARÍAS TOR[illegible]

SECRETARÍA DE EDUCACIÓN PÚBLICA
INSTITUTO POLITÉCNICO NACIONAL
CENTRO DE INVESTIGACIONES ECONÓMICAS ADMINISTRATIVAS Y SOCIALES

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México el día 30 del mes de noviembre del año 2010, el (la) que suscribe Oscar Raúl Ortega Pacheco alumno (a) del Programa de Maestría en Política y Gestión del Cambio Tecnológico con número de registro B081978, adscrito a Centro de Investigaciones Económicas, Administrativas y Sociales, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección de Raúl Vázquez López y cede los derechos del trabajo intitulado Gestión de la seguridad de la información en la empresa, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección Lauro Aguirre 120, Col. Agricultura, C.P. 11360, Delegación Miguel Hidalgo, México, D.F. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Oscar Raúl Ortega Pacheco

Agradecimientos

Han pasado más de dos años desde el momento en que decidí ingresar a la Maestría en Política y Gestión del Cambio Tecnológico y hoy puedo ver finalizado un ciclo en el que se obtuvieron grandes aprendizajes que fortalecen mi desarrollo como persona y como profesional.

Al hacer un análisis de este periodo no puedo evitar agradecer a aquellas personas que con su apoyo, ejemplo y comprensión me han impulsado a alcanzar diferentes metas.

En primer lugar mi más profundo agradecimiento al Instituto Politécnico Nacional, el cual ha formado parte de una piedra fundamental en mi vida diaria y de la cual siento gran orgullo y respeto.

A mis profesores de CIECAS, en especial a la Dra. Hortensia, Dr. Rubén, Dr. Humberto, Mtra. Aída y al Mtro. Jesús, quienes compartieron sus diferentes experiencias y conocimientos para adentrarnos en las diferentes temáticas involucradas en la maestría, pero que gracias a su ejemplo, consejo y dedicación me permitieron encontrar el balance entre mi vida personal, académica y laboral, al mismo tiempo que me permitieron desarrollar habilidades para considerar las consecuencias de ciertas decisiones que van más allá de lo tecnológico.

No podría entender el desarrollo del presente trabajo sin el apoyo del Dr. Raúl Vázquez quien a pesar de la distancia no dudó en brindar su espacio y tiempo para escuchar y analizar mis diferentes problemáticas y dudas, y con ello orientarme para poder alcanzar los objetivos planteados.

A mis amigos de la maestría pues aprendimos a escucharnos y a entender las distintas posiciones al momento de analizar situaciones de la vida cotidiana. Muy en especial a Martín y Alejandro a quienes considero un ejemplo a seguir en mi desarrollo humano y profesional.

A mis amigos de toda la vida que han hecho que este periodo sea de gran alegría y en quienes encuentro apoyo y comprensión.

Parte fundamental para ver consolidado este esfuerzo ha sido el constante apoyo de Fer y Lucy, compañeras de trabajo a quienes estimo y admiro. También a Marco y Pablo quienes me han facilitado el ejercicio de mis actividades profesionales con las académicas y que me han asesorado en el desarrollo del presente trabajo.

Finalmente, mis más grande agradecimiento, respeto y admiración para mis padres y hermana pues son la base de la persona que soy y gracias a su ejemplo he encontrado la confianza para afrontar los diferentes retos de la vida.

Dedicatoria

A mi sobrino Yoshuell Ortega.

Contenido

Índice de Tablas

Índice de figuras

Glosario

Cómputo forense. Aplicación de técnicas de análisis e investigación computacional con el objetivo de obtener elementos digitales (evidencia digital) que puedan utilizarse en un proceso legal (Robbins, 1998). Computación forense es el proceso de identificar, preservar, analizar y presentar evidencias digitales en una forma que sea legalmente aceptada (McKemmish, 1999).

Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso (ISO, 2007).

Correo no deseado o *spam*. Mensajes de correo electrónico no solicitado.

Cómputo en la nube (*Cloud computing*). Conjunto de servicios disponibles en Internet que cumplen con características de alta disponibilidad, crecimiento sea rápido y flexible, una gran cantidad de aplicaciones y que sea un servicio administrable y medible (CSA, 2009).

Cracking. Conjunto de técnicas empleadas para codificar, analizar y estudiar los principios de un programa sin disponer de su código fuente.

Datos. Una colección de hechos que es preciso procesar para que sean significativos (Pressman, 2002).

Dato personal. Toda información concerniente a una persona identificada o identificable (LFPDP, 2010)

Dato personal sensible. Datos personales que afectan la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave (LFPDP, 2010).

Delitos informáticos. Actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como un instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio (concepto típico) (Téllez, 2004).

Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados (ISO, 2007).

Divulgación de información. Publicar o dar a conocer información a alguien no autorizado para conocerla

Documento. Cualquier cosa que sirve por sí misma para ilustrar o comprobar por vía de representación un hecho cualquiera o la exteriorización de un acto humano (Parra, 2000).

Elevación de privilegios. Obtener privilegios sin autorización

Evidencia digital. Es un tipo de evidencia física. Esta construida de campos electromagnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales (Casey, 2000).

Evidencia Física. Cualquier objeto que pueda establecer que un evento ha ocurrido o provea orientación entre el delito y la víctima o entre la víctima y el sospechoso (Saferstein, 1998).

Gusano (*Worm)*. Código malicioso autopropagable el cual puede distribuirse a sí mismo a través de una conexión de red. Puede tomar acciones dañinas tales como consumir recursos de sistemas de red o locales, causando posiblemente un ataque de negación de servicio (UNAM-CERT, *s.f.*).

Información. Asociación de hechos (datos) en un contexto dado (Pressman, 2002).

Informática. Conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información (Téllez, 2004).

Ingeniería social. Conjunto de acciones no técnicas por las cuales se obtiene información correspondiente a un sistema por parte de los usuarios que tienen acceso legitimo a él, por lo general a través del uso de engaños. (UNAM-CERT, *s.f.*)

Integridad. Garantía de la exactitud y completitud de la información y los métodos de su procesamiento (ISO, 2007).

Keylogger. Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos lo que ha escrito el usuario afectado (información introducida por teclado: contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas. (UNAM-CERT, *s.f.*)

Malware. Proviene de una agrupación de las palabras *malicious software*. Este programa o archivo, que es dañino para el equipo, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí (UNAM-CERT, *s.f.*).

Negación de servicio distribuida (Distributed denial of service, DDoS). Es un tipo especial de ataque de negación de servicio desarrollado a través de múltiples equipos comprometidos sobre un mismo objetivo (Bennett, 2000).

Negación de servicio o denegación de servicio (Denial of Service, DoS). Actividad desarrollada por algún atacante con el objetivo de prevenir que usuarios legítimos tengan acceso a un recurso dado (CERT, 1997).

Negación de servicio. Negar o degradar el servicio a alguien.

Pharming. Acto de explotar una vulnerabilidad en el software de un servidor de DNS, que permite que una persona se adueñe del dominio de un sitio y redirija el tráfico hacia otro (UNAM-CERT, *s.f.*).

Phishing Scam. Es un conjunto de técnicas y mecanismos empleados por los intrusos o hackers con el propósito de robar información personal de un usuario y así poder Suplantar su Identidad (UNAM-CERT, *s.f.*).

Repudio. Negar una acción realizada

Robo de identidad. Ocurre cuando alguien utiliza información personal de un tercero sin su autorización para cometer fraude u otros delitos (FTC, *s.f.*).

Seguridad informática, en cómputo, de la información. Conjunto de técnicas centradas en la identificación y evaluación de riesgos potenciales que pueden producir un impacto en la confidencialidad, disponibilidad o integridad de la información.

Sniffer. Programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. (Téllez, 2004)

Spoofing. Conjunto de técnicas que tienen por objetivo engañar a una computadora o persona a través del robo de identidad.

Spyware. Programa espía y comúnmente se refiere a aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario (UNAM-CERT, *s.f.*).

Tampering. Modificación de datos o códigos

Troyano o Caballo de Troya. Programa de computadora que aparenta tener una función útil, pero que contiene código posiblemente malicioso para evadir mecanismos de seguridad, a veces explotando accesos legítimos en un sistema (UNAM-CERT, *s.f.*).

Virus. Un programa informático que puede infectar a otros programas modificándolos para incluir una, posiblemente encubierta, copia de sí mismo (Cohen, 1984).

Resumen

Es innegable el hecho de que las tecnologías de información y comunicaciones (TIC) han cambiado nuestro modo de vida, pues mediante el uso de diversas herramientas podemos efectuar actividades a gran velocidad y a menor costo. Si bien ya nos hemos acoplado a gran parte de estos cambios, muchos gobiernos y organizaciones han comenzado a preocuparse por los efectos adversos que se han derivado a partir de su uso. Nos referimos en particular a los delitos informáticos y al mal manejo que puede sufrir la información, situaciones que generan pérdidas millonarias a las empresas.

El presente documento presenta una serie de acciones aplicadas a un modelo de gestión de la seguridad de la información que permite alinear los objetivos de una empresa con las metas que se requieren para la protección de la información. Para lo cual partimos de la construcción de un modelo de gestión de la información que permite explicar el flujo completo que sufren los datos dentro de una empresa. Posteriormente se describen los diferentes modelos de gestión de riesgo informático donde se analizan sus principales ventajas y desventajas. Finalmente, partiendo de la base del modelo propuesto por Kiely y Benzel (2009) se establecen diferentes medidas que una empresa puede aplicar desde sus políticas, gobierno corporativo, elementos técnicos y de cultura para minimizar el riesgo informático. Así mismo se sugiere trabajar a futuro en la construcción de indicadores de seguridad, evaluar la validez del modelo presentado ante nuevos retos tecnológicos y desarrollar estudios de trayectoria tecnológica en cuanto a delitos electrónicos como innovación en elementos de seguridad.

Abstract

It is an undeniable fact that information and communication technologies have changed our way of life by providing tools that help us to reduce costs and time in traditional activities. At this time, we have already involved to many of these changes, but many governments and organizations have begun to worry about its negative effects. In particular the computer crimes and misuse of information, because these situations generate millionaire losses to businesses.

This document presents actions applied to an information security model that aligns the company objectives with the targets required to protect information. The first part describes an information management model that explains the different phases of the data flow in a business process. Subsequently, different risk management models were analyzed by discussing their advantages and disadvantages. Finally, using the Kiely and Benzel (2009) model, technical, cultural and governance actions are recommended to minimize information risks.

This work also suggests for future investigations the construction of information security indicators, to assess the validity of the model in according to the new technological challenges, and to develop studies of technological trajectory referred to cybercrimes.

Introducción

Es innegable el hecho de que las tecnologías de información y comunicaciones (TIC) han cambiado nuestro modo de vida, facilitando actividades que anteriormente habrían necesitado gran inversión de tiempo y recursos. Pero no sólo bastó su introducción para generar beneficios a las empresas y a la sociedad, pues requirió de una etapa de aprendizaje y optimización en la adopción de la tecnología. Si bien, como empresa o sociedad, ya nos hemos acoplado a gran parte de estos cambios, muchos gobiernos y organizaciones han comenzado a preocuparse por los efectos adversos que se han derivado a partir del uso de las TIC. Nos referimos en particular a los delitos informáticos, mismos que pueden derivarse de nuevas conductas o de la aplicación de los medios electrónicos para cometer otros delitos. Entre estos delitos podemos identificar el robo de identidad, la pornografía infantil, fraude, entre otros; situaciones que generan costos a empresas y particulares superiores a los 50 billones de dólares al año (Velasco, 2006).

Al día de hoy se han desarrollado diferentes tecnologías que permiten mitigar los riesgos asociados al uso de las TIC, sin embargo existe una mayor preocupación relacionada con el manejo de información y datos personales pues las TIC permiten el manejo de miles de millones de datos en cuestión de segundos, mismos que organizados e interpretados de modo adecuado constituyen un activo estratégico que permite a las organizaciones expandir sus mercados, desarrollar nuevos productos o servicios, o simplemente mejorar sus procesos.

Pero también su uso inadecuado puede convertirse en una desventaja si la información cayera en posesión de la competencia, además de que su mal manejo puede generar problemas que afecten la privacidad de una persona ocasionando desconfianza en los usuarios, la cual puede tener un impacto directo en las ventas de una empresa o en el desarrollo de una industria como puede ser el comercio

electrónico que a medida que crecen los niveles de confianza en el medio crecen los números de ventas.

Esto mismo ha desatado una discusión universal en relación a quién es el dueño de la información contenida en bases de datos que se encuentran en posesión de gobiernos o particulares y cuáles son las obligaciones de cada uno al momento de recibir y manejar datos. Como consecuencia se ha fomentado el desarrollo de políticas, procesos y tecnologías para su manejo, sin embargo una empresa debe balancear entre optimizar el flujo de datos, la utilidad y el valor de los mismos así como y la responsabilidad de protegerlos de pérdida, robo o mal uso, haciendo que la gestión de la seguridad de la información sea una actividad que permita alcanzar los objetivos empresariales.

En este contexto el presente documento explica el ciclo de gestión de la información para posteriormente establecer cuál es el valor de la misma dentro de una empresa. Se ha prestado especial importancia a la gestión debido a que ésta constituye la base para desarrollar una estrategia de seguridad, pues la primera acción que debe desarrollar una empresa es conocer el flujo completo de los datos y su valor con respecto al negocio, lo cual le permite obtener una visión clara de en qué actividades es necesario implementar políticas y tecnologías para la protección de los datos. Este proceso de gestión se analiza mediante cinco actividades básicas en toda gestión de datos: adquisición, selección, estructuración, modificación y eliminación.

En la primera sección se destacan los diferentes mecanismos con los que cuenta una empresa para adquirir datos y las acciones necesarias para convertirlos en información, conocimiento e inteligencia basados en el desarrollo de Páez (*s.f.*), quien presenta un enfoque basado en calidad contra cantidad de datos, pues para una empresa es importante poder contar con los datos adecuados en el momento preciso para la toma de decisiones. Así mismo se realiza un estudio de los principales riesgos informáticos que enfrenta la gestión de la información y la

situación actual sobre los ataques y acciones desarrolladas por empresas a nivel mundial.

En la segunda sección del trabajo se exponen los diferentes modelos para la gestión del riesgo informático que determinarán cómo identificar los riesgos y su nivel de impacto a nivel organizacional. En este punto es importante acotar que todos los modelos planteados buscan la minimización de riesgos y no son dependientes del manejo de una tecnología en particular, pues independientemente de la plataforma de hardware o software que se emplee existen los mismos riesgos potenciales para la gestión de la información.

En particular se desarrolla la descripción del modelo de gestión sistémica de la seguridad informática propuesto por Kiely y Benzel (2009) y Oliver, Allard, Antonsson, Bahl, *et. al.* (2009) que establece un modelo de cuatro nodos interrelacionados que facilitan la alineación de objetivos organizacionales con la estrategia de seguridad.

El capítulo 3 parte del modelo de Kiely y Benzel (2009) para establecer recomendaciones puntuales sobre acciones a desarrollar en una empresa para cada uno de los nodos. Este modelo se ha seleccionado debido a que es la primera propuesta de gestión de seguridad que considera un análisis sistémico donde cada acción tiene un efecto sobre otra, lo que permite establecer un equilibrio entre las políticas empresariales, los elementos tecnológicos, los procesos y los recursos humanos.

La primera parte del capítulo tres describe las acciones mínimas que a nivel estratégico deben ejecutarse en una empresa, básicamente el establecimiento de una estructura de gobierno para el manejo de información que se basa en el desarrollo de políticas que minimicen los riesgos pero que al mismo tiempo maximicen el valor de los datos. Estas definiciones pueden impactar en la ejecución de los procesos o en la estructura misma de la organización como puede ser mediante la creación de un área de seguridad.

En la segunda parte de éste capítulo se presentan las acciones necesarias para tomar una decisión en función de los riesgos existentes en un proceso de negocio ya sea mitigarlo, transferirlo o aceptarlo en función de un ejercicio de análisis de riesgos, para lo cual se hace uso del ejemplo de una empresa que desarrolla eventos corporativos. Es importante destacar que la información fue tomada de una empresa existente pero que para mantener su privacidad se utilizó el nombre de Eventos Premier. Posteriormente se analizaron los tipos de tecnología que permiten la gestión de los datos a fin de dar una recomendación sobre qué elementos mínimos deberá buscar un administrador de seguridad en la tecnología que ocupe dentro de su organización. Finalmente se hace un análisis de las acciones en materia de recursos humanos sobre la gestión de la información dando especial importancia a campañas de sensibilización y controles establecidos desde la política empresarial en esta materia.

Como parte de las conclusiones se manifiesta el hecho de que el establecimiento de controles para mitigar riesgos informáticos puede aportar ventajas competitivas, permitir el ahorro de recursos o facilitar el alcance de objetivos para diversas áreas de negocio al reutilizar la información para otros procesos. Así mismo se sugiere que para mantener un buen control de las acciones implementadas en seguridad se establezca un mecanismo de seguimiento, por lo que la organización deberá desarrollar indicadores de evaluación de acuerdo a sus políticas.

Capítulo 1. Gestión de la información

"... en la antigüedad, el hombre occidental quería ser sabio;
luego el hombre moderno quiso ser conocedor;
el hombre contemporáneo parece contentarse con estar informado
(y posiblemente en el hombre futuro no esté interesado en otra cosa que en tener datos)."

Irsaet Páez Urdaneta

Hoy en día, la información dentro de las organizaciones se ha convertido en un activo fundamental para establecer ventajas competitivas en su desarrollo (Brown, 2006). Sin embargo para su óptimo uso se requiere de un manejo adecuado, de establecer sistemas que puedan gestionarla y convertirla en conocimiento útil para la empresa o para sus empleados, pues es importante recordar que los datos y la información por sí mismos no constituyen un valor, pero sí lo adquieren cuando su interpretación permite generar mejoras a sus procesos de negocio (Curbelo, *s.f.*).

Este planteamiento se ha visto reforzado a partir del uso de las tecnologías de información y comunicaciones, pues su uso permite el procesamiento de millones de datos de diferentes localidades en cuestión de segundos. En este sentido y previo a analizar cómo se adquieren y manejan datos dentro de las organizaciones debemos definir el concepto de información.

1.1. Definición de la información

La información es un "conjunto de datos, estructurados y formateados" (Morales, 2004:1), los cuales pueden ser interpretados y manipulados o bien puede ser entendida como "un conjunto de datos, que pueden ser fácilmente codificados, y por lo tanto transferidos y aprovechados." (Bianco, Lugones, Peirano y Salazar, 2002).

Es en este sentido que Páez (*s.f.*) recurre al desarrollo de la pirámide informacional para explicar la correlación que existe entre la posesión de datos y el desarrollo de inteligencia, centrándose en una pirámide de cuatro niveles: datos, información, conocimiento e inteligencia (figura 1).

Fig. 1 Pirámide informacional

Fuente: Páez, *s.f.*

De la figura 1 podemos observar que los datos constituyen la base de la pirámide informacional, los cuales pueden interpretarse como una serie de símbolos, caracteres o palabras que por sí mismos carecen de significado. Por ejemplo podríamos tener una lista con números telefónicos, al tomar un dato cualquiera de la lista carecería de significado práctico pues la secuencia de números podría interpretarse como un número telefónico, un billete de lotería, folio de facturación y cualquier otra característica con la que se desee asociar.

Es en este punto donde encontramos el concepto de información, la cual se genera al asociar dos datos de manera estructurada. Siguiendo con el ejemplo si en la lista se indica que se refiere a números telefónicos y a su vez se asocian a un nombre y apellidos podemos inferir que cada número corresponde al teléfono de la persona correspondiente.

En consecuencia si podemos realizar una serie de conclusiones con respecto al conjunto de datos estructurados alcanzamos conocimiento, por ejemplo podríamos concluir luego de analizar la información que la lista se refiere a personas que viven en la ciudad de México. Sentando la base para la toma de decisiones, la cual constituye la inteligencia. Es decir, si contrastamos la lista de números telefónicos con una lista de clientes con los que cuenta una empresa, podríamos conocer cuántos clientes se encuentran en la ciudad y con ello formular

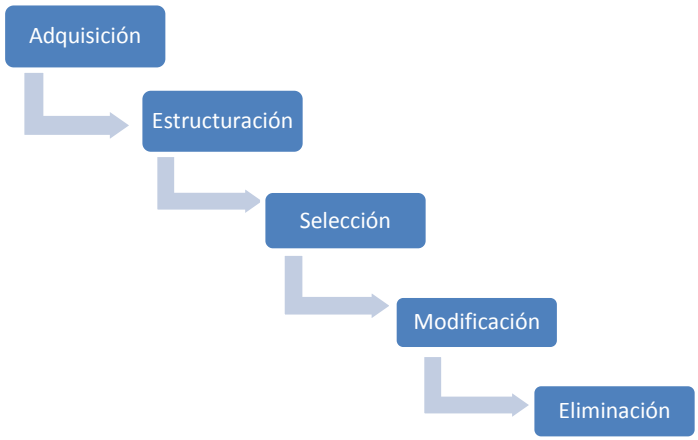
una estrategia para incrementar el número de clientes o realizar un servicio adicional en los ya existentes.

La principal característica de la propuesta de Páez es el hecho de que ante una gran cantidad de datos se aprovechan aspectos muy específicos que permiten tomar decisiones, *calidad vs. cantidad,* siendo el resultado del tratamiento de los datos el principal valor de la organización. Esto mismo ha representado el desarrollo de diversas disciplinas encargadas del diseño de información y con ello la instalación de normas y políticas que permitan proteger los datos estructurados.

1.2. Manejo de la información

Como lo hemos mencionado, alcanzar conocimiento o inteligencia requiere del manejo de los distintos tipos de datos. Una de las maneras de entender como se realiza éste tratamiento es a partir de una representación lineal de las operaciones básicas de los datos: adquisición, estructuración, selección, modificación y eliminación.

Fig. 2 Representación lineal del tratamiento de datos



Fuente: Elaboración propia

Cada una de estas operaciones se refiere a lo siguiente:

- Adquisición: Consiste en los diferentes mecanismos que puede ocupar una persona o empresa para la recolección de datos. Es importante para una empresa o persona tener un objetivo definido sobre el tipo y uso de los datos, pues llevar a cabo una recolección de datos sin la meta clara podría incrementar los costos de adquisición y almacenamiento.

- Estructuración: Retomar y acomodar los datos de manera que sirvan como guía de acción. Esto debe permitir que aquellas personas que tengan acceso a los mismos datos puedan interpretar el mismo mensaje, pues como lo especifica Paoli (1989) "dos sujetos tienen la misma información, no cuando tienen los mismos datos, sino cuando tienen el mismo modo de orientar su acción."

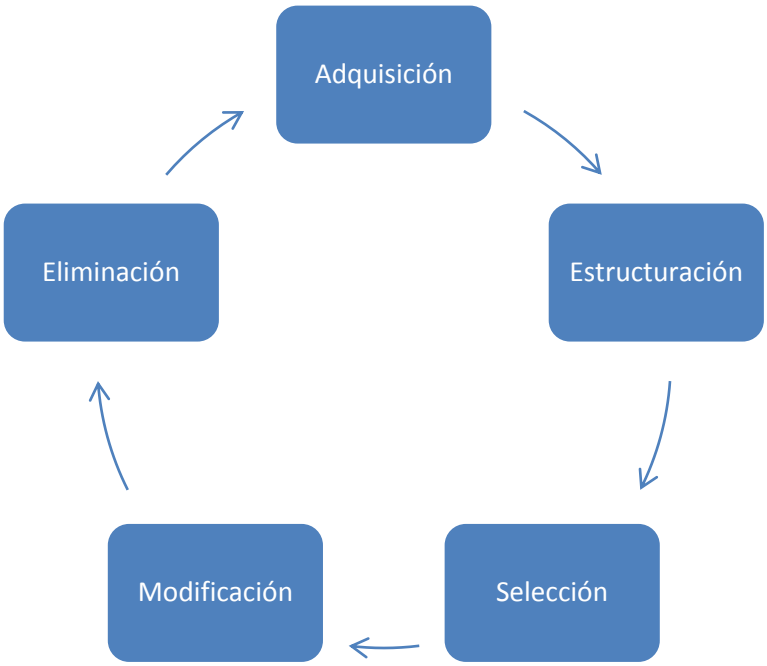
- Selección: Consiste en discriminar aquella información que no aporta ningún valor en el proceso al cual será asignada.

- Modificación: Contempla el proceso para la actualización y rectificación de los datos.

- Eliminación: Este proceso implica dos acciones, la destrucción definitiva de los datos y la reasignación de un grupo de datos a otros procesos de selección.

Debido a que este proceso es continúo y recibe información de diferentes fuentes y en momentos distintos debemos considerar que las acciones pueden iniciar en cualquier momento y no necesariamente en la adquisición pues la salida de un proceso puede representar la generación de nuevos datos (figura 3).

Fig. 3 Proceso circular de la gestión de datos



Fuente: Elaboración propia

Ahora bien, el manejo de datos a partir del uso del uso de las tecnologías ha provocado que algunas empresas y países se preocupen por el manejo que se da a los datos personales y quién es el dueño de los datos, esto con el afán de proteger a las personas del envío de información no deseada, robo de identidad, reputación, entre otros problemas derivados de un mal manejo. En el caso mexicano la Ley Federal para la Protección de Datos Personales en Posesión de Particulares (LFPD, 2010) exige a las empresas que para la gestión de datos se contemplen cuatro derechos fundamentales: Acceso, Rectificación, Cancelación y Oposición.

El primero de los derechos, *acceso*, se refiere a la capacidad que tienen los individuos para solicitar a un organismo toda la información que han recopilado acerca de su persona. En el caso de la *rectificación* se refiere a la capacidad del individuo para solicitar que su información sea modificada. En cuanto a *cancelación*, se entiende como el derecho que tiene una persona para que su información sea destruida. Finalmente, por *oposición* nos referimos a la capacidad

que tienen los individuos de oponerse ante qué hará una empresa con sus datos. A todo esto se debe resaltar que las empresas están obligadas a informar a los usuarios en el momento en que su información sea cancelada o se haya terminado el proceso de datos para los cuales fueron recopilados.

Estas recomendaciones o exigencias regulatorias que han realizado los diferentes organismos, representan al día de hoy una modificación en la gestión de datos de las empresas pues en el proceso anteriormente descrito debe de incorporarse la manifestación de los derechos de las personas en todo el proceso de tratamiento, generando una reevaluación sobre el valor que tiene la información.

1.3. El valor de la información

Anteriormente hemos mencionado que la información puede representar un valor para una empresa al grado de convertirse en un activo fundamental para la era actual. Sin embargo una de las principales dificultades que tiene la organización es poder establecer un valor económico para tomar decisiones acerca de su gestión.

Para ello es importante conocer los diferentes tipos de información con los que cuenta una empresa bajo la perspectiva del valor que representa para su operación:

- Información pública: comprende el conjunto de datos que la empresa genera para hacer de conocimiento público, principalmente para establecer una imagen corporativa y descriptiva acerca de sus servicios o productos, así como información de contacto y de otro tipo de que la empresa considera pertinente dar a conocer o que por regulación debe ser de uso público.

Esta información debe de manejarse de modo que pueda ser conocida por la mayor cantidad de personas posibles. En realidad su valor es equivalente al costo de su generación y, por su parte, el costo puede calcularse en relación a las horas hombre invertidas el personal para el desarrollo de la información, además de los costos asociados a la adquisición y selección de datos.

- Información privada/clasificada: Esta clasificación considera el conjunto de datos que la empresa utiliza para su operación interna, por lo general implica el número de ventas, clientes, situación financiera, número de empleados, estructura organizativa, secreto industrial, manuales de operación, entre otros. En este caso el valor de la información se calcula a partir del costo de generación de la misma pero además del costo que tiene en el mercado, es decir, el costo por el cual un competidor estaría dispuesto a pagar por ella. Desafortunadamente no es sencillo obtener el valor cotizado en el mercado pero existe un modo indirecto el cual se calcula a partir del nivel de ingresos obtenidos por una empresa derivados de la explotación de la información clasificada en un periodo de tiempo definido. Por ejemplo, para calcular el valor que tiene un manual de operación en una empresa podemos calcular su valor a partir de las ventas generadas por la organización y en las cuales se utilizó el procedimiento del manual durante un año o trimestre.

- Datos personales y dato personal sensible. El primero de ellos se refiere a "cualquier información concerniente a una persona identificada o identificable" (LFPDP, 2010:3). Mientras que el segundo se refiere a "datos personales que afectan la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave" (Deloitte, 2010:3). En esta clasificación el valor de la información suele ser muy alto y en ocasiones ignorado por las empresas pues estos no

necesariamente representan un eje central en sus procesos de negocio y por lo mismo no son analizados. Sin embargo en el mercado este tipo de datos alcanzan valores millonarios principalmente por su utilidad para la comisión de delitos derivados del robo de identidad. Para una empresa su principal preocupación puede centrarse en el costo derivado de una sanción económica o la pérdida de reputación y confianza que podría generar una mala gestión de estos datos.

Es precisamente por este valor económico que el número de incidentes de robo de información se han incrementado representando ingresos para el crimen organizado superiores a los 559 millones de dólares tan sólo en los Estados Unidos durante el año 2009 (IC3, 2009).

Siendo necesario para la gestión de la información conocer los principales ataques existentes y sus fuentes de origen para establecer una estrategia que permita resguardar este activo empresarial.

1.4. Riesgos asociados a la gestión de la información

Al analizar los diferentes riesgos que pueden poner en peligro a la información de una compañía es necesario retomar el hecho de que TIC juegan un papel fundamental, pues a pesar de que algunos de los riesgos han existido previo a la aparición de estas tecnologías, su incorporación ha incrementado el nivel de alcance y daño ocasionado, derivado de la cantidad de datos que pueden recopilarse o almacenarse.

Es por ello que antes de centrarnos en los riesgos asociados a la información revisaremos aquellos que se derivan del uso de las tecnologías de información.

- Abuso de los recursos: Ocurre cuando los usuarios de los equipos de cómputo utilizan los recursos de la organización para fines personales o cuando hacen uso innecesario de los servicios de cómputo.

- Fuga de información: Se refiere a la extracción no autorizada de información ya sea por personal interno o externo. En este caso debemos tomar en cuenta que la información puede ser sustraída por medios extraíbles como memorias usb, cd's, etcétera o también haciendo uso de las redes de información, correo electrónico o sistemas de mensajería instantánea y redes sociales.
- Correo electrónico no deseado: "Este tipo de correo es un problema en general pues gran parte del tráfico en la red corresponde a este tipo de correos, además de que su contenido podría incluir códigos maliciosos o vínculos a sitios con contenidos inapropiados o peligrosos para el equipo. En las empresas el correo no deseado, o *spam,* trae consigo otro problema pues debido a que los usuarios reciben gran cantidad de *spam* invierten parte de su tiempo laboral para eliminar estos correos" (Navega Protegido, 2009). Este riesgo es uno de los 10 más importantes alrededor del mundo, pues actualmente más del 90% de los correos que existen en Internet corresponden a esta clasificación.
- Ataques informáticos: "En Internet existen usuarios malintencionados que se dedican a realizar ataques contra la infraestructura de cómputo de la organización, estos ataques pueden tener varios objetivos y principalmente identificamos los siguientes" (Navega Protegido, 2009):
    - Robo de información
    - Negación de servicio. Conocido también como DoS por sus siglas en inglés. "Este ataque se desarrolla con el objetivo de evitar que los usuarios o clientes de la compañía accedan a los servicios ofrecidos, sea comercio electrónico o simplemente acceso a la información ofrecida en su portal." (Navega Protegido, 2009)
    - Daño a la reputación.
    - Uso de recursos. "Algunos intrusos informáticos aprovechan los recursos de la compañía para llevar a cabo otros ataques, por ejemplo un atacante podría utilizar el almacenamiento de un servidor

para guardar gran cantidad de software malicioso, disminuyendo la capacidad de almacenamiento para la información de la compañía." (Navega Protegido, 2009).

- Códigos maliciosos: "Los códigos maliciosos son programas que tienen el objetivo de ocasionar algún daño en el equipo de cómputo o en la información, en general se convierten en un problema en las organizaciones pues afectan el rendimiento de los equipos, además de que algunos de ellos permiten acceder información confidencial o abrir alguna puerta para que los intrusos informáticos puedan tomar control total del equipo." (Navega Protegido, 2009).

La mayoría de estos ataques informáticos tienen éxito debido a que se utilizan técnicas que logran persuadir a los usuarios de realizar acciones en perjuicio del equipo o de la organización y en muchas ocasiones los trabajadores no están conscientes del daño ocasionado, a esto se le conoce como ingeniería social y puede ser considerado como el principal peligro dentro de las organizaciones.

Ahora bien, retomando las diferentes etapas de la gestión de información podemos identificar los siguientes riesgos:

Robo de información

Ya anteriormente describimos el significado de la fuga o robo de información por lo que a continuación se describirá de modo detallado el modo en que la información puede ser extraída.

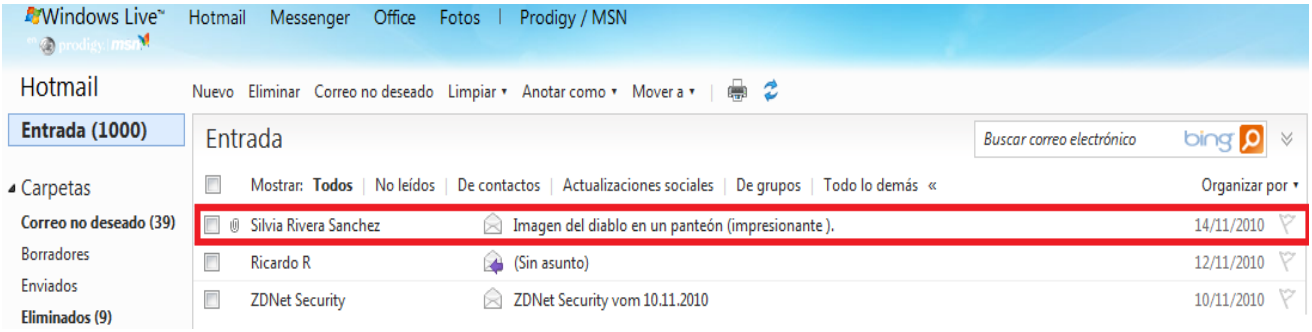
1) Extracción de información por medios extraíbles (USB, disco duro, disquetes). Esta actividad ocurre cuando los empleados extraen archivos de la compañía en dispositivos extraíbles.
2) Envío de información por servicios de mensajería. En ocasiones la información no tiene que salir físicamente del lugar, pues el correo electrónico, la mensajería instantánea, redes sociales y otras herramientas

de comunicación permiten enviar datos digitales a otras partes del mundo, pudiendo así extraer información de la compañía sin el uso de dispositivos de almacenamiento externos.

3) Extracción de información mediante la red de datos. Las redes de datos permiten compartir información entre los componentes de una organización, sin embargo si un usuario externo pudiera tener acceso a la red podría tener acceso a la información que se comparte, pudiendo así extraer los datos de la organización.
4) Extracción de datos mediante códigos maliciosos. El uso de códigos maliciosos es probablemente el método más complejo de extracción de información, pues dicho proceso comienza con el desarrollo de un programa computacional capaz de obtener información, ya sea a través de la recopilación de datos existentes o a través de la recopilación de la información generada por el usuario.

   De tal modo que una vez desarrollado el software espía, el siguiente paso será desarrollar una estrategia para lograr que el programa se introduzca en el equipo que desea obtener la información, usualmente la ingeniería social es el método más efectivo, pues es un tipo de ataque que explota el conocimiento del comportamiento humano para conseguir un propósito específico, por ejemplo un atacante podría enviar un correo electrónico con un archivo malicioso adjunto y para lograr que un usuario lo abriera en su computadora podría bastar con una frase en el asunto donde se manejara un tema de interés actual o que se aproveche de la curiosidad de las personas para que descarguen el documento adjunto, como en el caso de la siguiente figura en la que se utiliza un tema de interés general (el diablo) para provocar que los usuarios abran el correo electrónico.

Fig. 4 Ingeniería social en correo electrónico



Fuente: Elaboración propia

Una vez que se ha logrado que el programa se instale en el equipo, la siguiente fase será garantizar que el software logre ocultarse hasta que la información deseada sea extraída. Una gran ventaja de esta técnica es que a partir de la infección de un equipo en una red es posible propagar la infección para poder obtener mayor cantidad de datos.

Pérdida de información

La pérdida de información digital por parte de las organizaciones puede ocurrir por la acción intencional de un usuario o programa que elimina información, como también de modo accidental donde puede ocurrir por el error de un usuario o una falla técnica en el equipo de cómputo que pueda volver inaccesible la información. En ambos casos es indispensable que las organizaciones mantengan una copia de la información crítica.

Suplantación de identidad

Los casos de suplantación o robo de identidad pueden analizarse bajo dos perspectivas, la primera con el objetivo de obtener mayor cantidad de datos cuando piratas informáticos logran convencer a otros usuarios de que les entreguen información confidencial haciéndose pasar por otra entidad de confianza, como ocurre con el *phishing* y *spear phishing*. En el otro caso se puede

utilizar el robo de identidad para desviar recursos económicos de una fuente a otra.

Ataques de negación de servicio

Uno de los principios fundamentales de la seguridad de la información es la *disponibilidad*, la cual se refiere a que los usuarios deben acceder a la información en el momento que sea necesario siempre y cuando se tengan los permisos correspondientes. De tal modo que provocar que la información no esté disponible puede provocar retrasos en el proceso de desarrollo de un nuevo producto. Esta actividad de negación de servicio puede ocurrir por alguno de los siguientes métodos:

- Códigos maliciosos. Los códigos maliciosos pueden ocasionar una negación de servicio a través de la eliminación o cifrado de la información.
- Errores de configuración en el software. En ocasiones algunos programas de cómputo mantienen en sus configuraciones reglas sobre cómo actuar ante ciertas circunstancias, por ejemplo ante la falta de espacio de almacenamiento en disco duro, dichas reglas pueden generar que la información no sea disponible si no son configuradas de manera adecuada.
- Error humano. Uno de los problemas más comunes en la administración de la seguridad de la información se deriva del manejo de una gran cantidad de herramientas, pues a pesar de su existencia, la información puede no ser accesible debido a errores humanos como la desconexión accidental de un servidor o el cierre de una aplicación por falta de una correcta programación.

1.5. Situación actual de riesgos informáticos

Si bien hemos mencionado anteriormente que la cantidad de riesgos se ha incrementado conforme se han desarrollado las tecnologías de información hasta el

momento no hemos establecido claramente cómo ha evolucionado este proceso para conocer la situación actual que viven las organizaciones.

Para analizar cómo han evolucionado los ataques informáticos y sus motivaciones podemos dividirlo en dos grandes periodos, el primero de 1960 a 1999 y el segundo desde 1999 al día de hoy, la razón principal es que durante el primer periodo se desarrollaron tecnologías que comprometieron sistemas de cómputo de manera accidental y otras con la principal motivación de obtener un reconocimiento internacional en el área de cómputo. Es en este periodo donde encontramos amenazas como NATAS, un virus computacional de gran impacto en América Latina, cuyo principal propósito era dañar el sector de arranque de los disquetes dificultando su lectura y en muchos casos ocasionando la pérdida de información para personas u organizaciones que no contaban con expertos capaces de recuperar la información. También podemos encontrar personajes sobresalientes como Kevin Mitnick o John Draper que lograron irrumpir en sistemas de cómputo y telefonía de grandes organizaciones como el Pentágono o AT&T.

Si bien durante este periodo se ocasionó pérdidas económicas o de imagen a las empresas debemos comprender esta etapa como el desarrollo y adaptación de las nuevas tecnologías, además de que no se tenía bien identificado el impacto que podría suceder para una persona, empresa, comunidad o país.

La presencia de este tipo de riesgos y el incremento en el número de incidentes alrededor del mundo ha motivado a investigadores y gestores de las TIC a desarrollar diferentes técnicas para la protección de la información, las cuales van desde el uso de soluciones basadas en tecnología (firewalls, antivirus, antispyware, etc.) a modelos de gestión que respondan a los objetivos corporativos (ITIL, COBIT, ISO 27001, etc.).

El año 1999 marca una separación en los periodos y en los tipos de ataque pues es en este año que las diferentes tecnologías alcanzan plena madurez y dejan de actuar por separado, es decir en este periodo se comienza a observar ataques con tecnologías o comportamientos integrados, por ejemplo los virus computacionales comenzaron a tener comportamientos similares a los de un programa espía o bien se han ocupado como parte de los ataques de phishing. La consolidación de este tipo de tecnologías se puede observar en el ataque de negación de servicio desarrollado contra los servidores de Yahoo, Aol, Microsoft y otras organizaciones dejando incomunicados y sin servicio a millones de usuarios en la red. Siendo la primera vez que un ataque informático tiene una consecuencia económica y social.

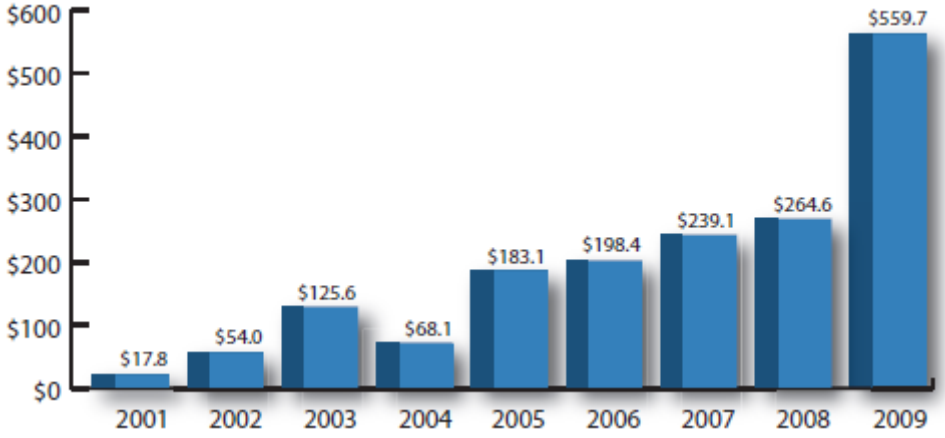
En ese mismo año tuvimos la aparición de Melissa, un gusano informático capaz de aprovechar vulnerabilidades en el sistema Word, cuyos daños se estimaron en los 350 millones de dólares. Debemos entender que en este periodo (1999 – al día de hoy) además del grado de madurez de las tecnologías también se incrementó el número de usuarios de las TIC a nivel mundial ocasionando que los daños fueran mucho mayores.

Durante esta etapa posterior a 1999 es que surgen movimientos políticos en la red teniendo consecuencias importantes, por ejemplo en el caso de las elecciones de los Estados Unidos donde se atribuye el éxito del presidente Barak Obama al desarrollo de una estrategia de marketing basada en el manejo de Internet y las redes sociales. Pensando en el caso mexicano las redes sociales han logrado influir en la toma de decisión de algunos legisladores, pues en el año 2009 se estableció una propuesta para incorporar un nuevo impuesto a las telecomunicaciones el cual podría haber afectado el desarrollo de internet por lo que a través de la red social Twitter se generaron más de 100 mil protestas en menos de 48 horas obligando a los legisladores a eliminar la propuesta. Esto tiene especial relevancia en relación con los riesgos informáticos porque bajo la

influencia política que tienen las TIC, se han desarrollado ataques informáticos a infraestructuras de cómputo de gobierno en señal de protesta, mismas que han tenido una repercusión en cuanto a imagen, pero también con consecuencias económicas como los ataques ocasionados a Estonia en año 2007.

Recientemente y de acuerdo al reporte del año 2009 del *Internet Crime Complaint Center* los delitos informáticos han ocasionado pérdidas a las organizaciones de manera sostenida, pues tan solo en el año 2000 las pérdidas económicas derivadas de estos ataques correspondían a 17.8 millones de dólares, mientras que para el año 2009 las perdidas se estimaron en 559 millones de dólares, un crecimiento de 3140%. A continuación se muestra la gráfica de pérdidas ocasionadas para los últimos nueve años.

Fig. 5 Pérdidas anuales ocasionadas por delitos electrónicos



Fuente: IC3, 2009

Es interesante observar que en el año 2009 las pérdidas crecieron al doble con respecto al año 2008, situación que podría explicarse a partir del hecho que las empresas disminuyeron sus presupuestos a las áreas de TI como consecuencia de la crisis económica mundial. No es propósito de la presente tesis explicar dicho comportamiento sin embargo se recomienda analizarlo a detalle pues además de

ésta situación se inició un crecimiento acelerado del uso de servicios en la nube y la incorporación de nuevas tecnologías y tendencias de ataques.

De acuerdo a la Asociación Colombiana de Ingenieros en Sistemas, quienes desde el año 2008 realizan una encuesta de seguridad informática para América Latina, los riesgos identificados con el manejo de la información son (Cano, 2009):

- El 60% de las empresas registra abuso de recursos bajo el concepto de instalación de software no autorizado.
- El 30.9% de las empresas ha sufrido de accesos no autorizados a sus sistemas de cómputo.
- El 70.9% ha sufrido de incidentes derivados de códigos maliciosos
- El 9.9% asegura haber sufrido robo de datos
- 4.8% Pérdida de la integridad de la información
- 19.5% Pérdida de información
- 15% Tuvo ataques de negación de servicio
- 13.5% Sufrió de ataques de suplantación de identidad

Por su parte Deloitte (2009) asegura que a nivel mundial la pérdida o fuga de información se da en el 65% de los casos por modo accidental (pérdida o robo de equipo de laptops, memorias USB, CD 's, entre otros).

Estos datos tienen especial relevancia pues es a partir de esta información que las empresas toman decisiones respecto de su seguridad y les permite establecer una comparación con respecto a otras organizaciones. En este mismo sentido Ernst & Young (2009) nos indica que a pesar de que apenas el 8% de las empresas han implementado un sistema de gestión de la seguridad de la información, el 32% considera dentro de sus planes formalizar y certificar sus sistemas de seguridad.

En relación a lo anterior debemos preguntarnos cómo gestionamos la seguridad de la información pues en más del 60% de las empresas se han implementado soluciones tecnológicas relacionadas con algún riesgo en particular y sólo el 25%

cuenta con políticas bien establecidas que integren el modo de interacción entre los sistemas y las personas.

Finalmente, el presente trabajo cuenta con información reciente y que maneja una metodología que no se basa en el uso de una tecnología en particular, sin embargo será necesario evaluar su aplicación presente y futura a partir de las nuevas tendencias de riesgos y los retos que el *cómputo en la nube* ha introducido, pues los niveles de exposición al riesgo, así como la privacidad y disponibilidad de la información ya no dependerán de una empresa en particular.

Estos nuevos retos derivados de la distribución de los datos y del cumplimiento regulatorio son analizados en las conclusiones del presente trabajo.

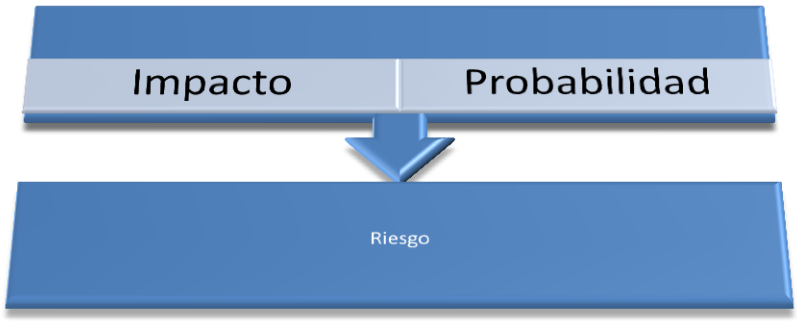
Capítulo 2. Gestión del riesgo informático

En los últimos años las tecnologías de información y comunicaciones y se han introducido en los diferentes sectores industriales convirtiéndose en un elemento clave para la mejora de procesos en las organizaciones, pues una de sus características más importantes es que las TIC y en particular las computadoras permiten manejar grandes volúmenes de información en menores tiempos. Esta creciente tendencia en su uso y debido a sus diferentes aplicaciones ha permitido el surgimiento de diferentes riesgos que están directamente asociados a su uso. Esto no significa que los riesgos existan sólo por el uso de las TIC, pues las organizaciones enfrentan a diario una serie de riesgos que pueden poner en peligro la estabilidad y continuidad del negocio, los cuales pueden llevarse a cabo en cualquier área de la organización, por ejemplo los riesgos financieros. De tal manera que las organizaciones definen diferentes estrategias para hacer frente a estos peligros a fin de continuar con su operación.

En particular los riesgos informáticos están vinculados con el manejo de información de la organización en medios digitales, pero antes de hablar del riesgo informático es importante definir que es un riesgo:

- "Aquella eventualidad que imposibilita el cumplimiento de un objetivo" (Sena y Tenzer, 2004).
- "Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias. (…) en algunas circunstancias el riesgo surge de la posibilidad de que ocurra algún cambio ante un evento o resultado esperado. " (ISO, 2007) Gráficamente podemos visualizar el riesgo de la siguiente manera:

Fig. 6 Componentes de un riesgo



Fuente: Microsoft, 2006

- "Es la exposición a una situación donde existe incertidumbre" (Holton, 2004).

De lo anterior podemos observar que un riesgo ocurre ante una situación no esperada y que podría afectar al cumplimiento de algún objetivo. Por otro lado recordemos que, como lo indica Jose Antonio Castro, Director de seguridad informática de Santander Central Hispano, el "riesgo está presente en la mayoría de las actividades de la empresa, desde el lanzamiento de un nuevo producto hasta la concesión de un crédito, y de su adecuada gestión depende en gran parte el cumplimiento de los objetivos; por ello es importante calibrar los riesgos tecnológicos en función de los objetivos de negocio" (Castro, 2002:46), siendo la gestión del riesgo la encargada de proteger los objetivos del negocio estableciendo medidas que permitan disminuir los niveles de exposición ante un riesgo.

En informática, la gestión del riesgo puede entenderse como un proceso cíclico que busca minimizar el impacto de un incidente de seguridad informática, el cual se presenta cuando la información se he visto comprometida en uno de los siguientes principios:

- Confidencialidad: "Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso" (ISO, 2007).
- Integridad: "Garantía de la exactitud y completitud de la información y los métodos de su procesamiento" (ISO, 2007).
- Disponibilidad: "Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados" (ISO, 2007).

Es importante resaltar que la gestión del riesgo y en consecuencia la gestión del riesgo informático permiten a la compañía garantizar la continuidad en cada uno de los procesos de la organización y en algunos casos podría permitir tomar decisiones asociadas a la inversión (Holton, 2004).

2.1. Modelos de gestión del riesgo informático

La gestión del riesgo informático tiene la particularidad de que debe permitir a las organizaciones implementar estrategias que permitan minimizar los riesgos, pues queda claro que no podemos hablar de un sistema completamente libre de vulnerabilidades, pero sí de un sistema que recibe el menor impacto ante una amenaza. Es por ello que se han desarrollado diversos modelos para la gestión del riesgo informático, donde se puede observar que la gestión debe ser un proceso cíclico y continuo para las organizaciones.

En una primera aproximación Sena y Tenzer (2004) propone el siguiente modelo de la figura 7:

Fig. 7 Modelo de gestión del riesgo

Fuente: Sena y Tenzer, 2009

Como lo indica la figura, este modelo consta de cinco etapas:

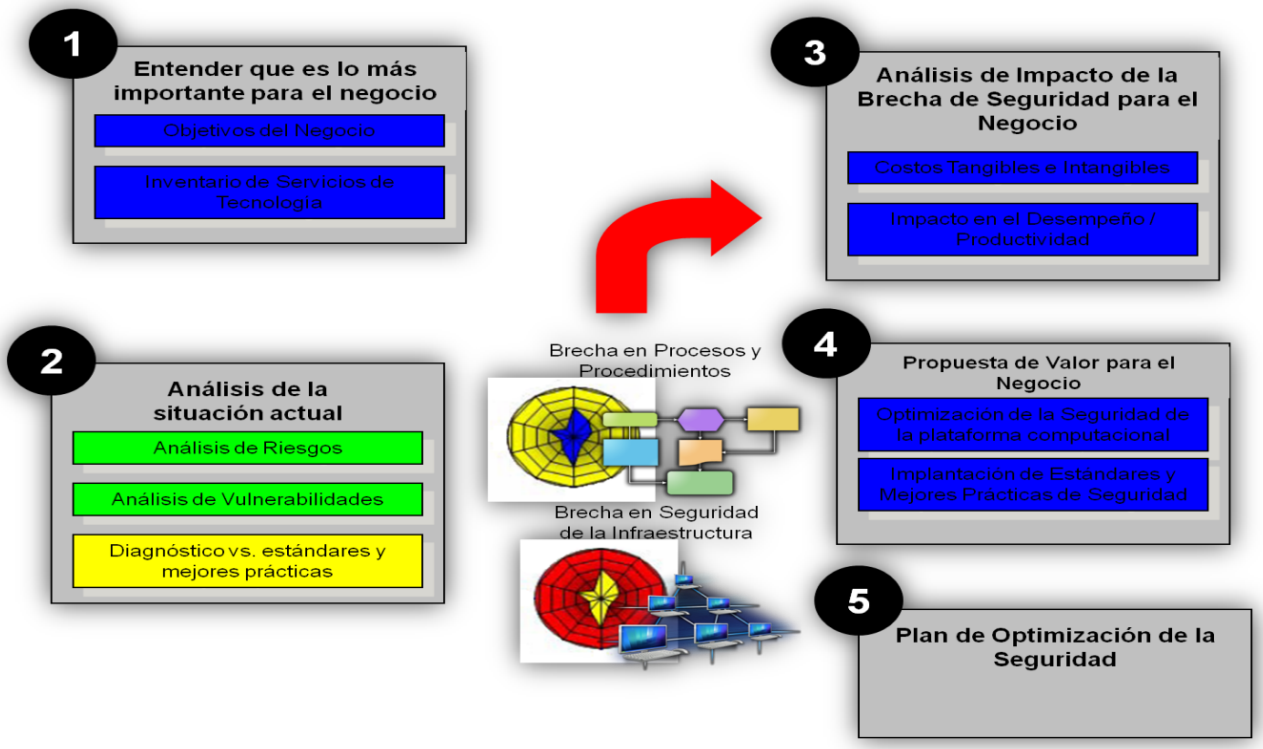
1) Identificación de riesgos. Este proceso consiste en identificar cuáles son las amenazas que podrían afectar el funcionamiento de la organización. En este proceso de identificación están comprendidos tanto los riesgos derivados del uso de la tecnología como los ocasionados por los usuarios de la tecnología.

2) Cálculo de exposición al riesgo. Este proceso consiste en emitir una aproximación probabilística que indique el nivel de exposición que tiene una organización o un proceso ante determinada situación.
3) Identificación de controles. En este punto se debe evaluar si existen controles o medidas implementadas para los riesgos existentes. Esto implica también una evaluación de la eficiencia de los controles implementados.
4) Calcular el riesgo residual. Resulta del cálculo del riesgo pero tomando en cuenta la aplicación de medidas preventivas.
5) Aceptación o rechazo del riesgo residual. En este punto la organización deberá tomar una decisión de acuerdo a los resultados del riesgo residual. En general, una vez obtenido el resultado la organización puede actuar de tres maneras distintas:
    a. Aceptar el riesgo. Esta decisión involucra que la organización esté consciente de la existencia de un riesgo, sin embargo la organización decide no implementar alguna medida para mitigarlo, ya sea porque la probabilidad de ocurrencia sea muy baja o porque el incidente no tiene un impacto sobresaliente en el desempeño de la organización.
    b. Mitigar el riesgo. Aquí la organización ha decidido aceptar el riesgo pero también ha optado por implementar algún mecanismo que disminuya su exposición al riesgo y por tanto su riesgo residual sea menor.
    c. Transferir el riesgo. Hay ciertas ocasiones en que la organización no puede mitigar el riesgo por sí misma, pero de acuerdo al nivel de exposición es probable que la organización deba transferir el riesgo, es decir optar porque otra organización sea quien mitigue los efectos de un incidente informático.

Otro modelo aplicado en la gestión de riesgos es el propuesto por Arbeláez (2008), el cual puede verse como una variante del modelo anterior, sin embargo

hace énfasis en que la gestión del riesgo debe estar alineada a los objetivos organizacionales (figura 8).

Fig. 8 Fases de la gestión del riesgo



Fuente: Arbeláez, 2008

Este modelo parte de un punto previo a la identificación de riesgos, el entendimiento del negocio, esto es muy importante pues el punto donde aplicación de la gestión de riesgos debe tener en claro la protección del proceso de negocio, convirtiéndose así en una herramienta clave que permita alcanzar los objetivos organizacionales. Un punto adicional a revisar en este modelo es que en el análisis del riesgo se toman en cuenta algunas herramientas de diagnóstico, al mismo tiempo que los estándares, mejores prácticas y regulaciones también son tomados en cuenta para determinar los riesgos existentes en la organización.

Por su parte Microsoft (2006) ha propuesto un modelo de gestión del riesgo de cuatro fases (fig. 9) tomando un enfoque cualitativo que permite identificar rápidamente los peligros existentes para posteriormente realizar un análisis cuantitativo que permita seleccionar aquellas amenazas a la seguridad que presenten el mayor impacto al negocio.

Fig. 9 Fases de la gestión del riesgo

Fuente: Microsoft, 2006

A continuación se describe cada una de las fases:

1) Evaluación del riesgo. Esta etapa consiste en la identificación de riesgos y en determinar una clasificación de su impacto con respecto al negocio. Las actividades que se involucran son las siguientes:

    - *Plan de recopilación de datos.* "Involucra el desarrollo de un plan que defina las áreas en las que se trabajará la gestión del riesgo y los mecanismos necesarios para recopilar los datos necesarios." (Microsoft, 2006:24).

- *Determinación de riesgos.* Se requiere de una detallada recopilación de los procesos para su análisis e identificación de amenazas al proceso (Microsoft, 2006).
- *Clasificación de riesgos.* "Desarrollo de métricas que permitan establecer prioridades para calificar y cuantificar los riesgos encontrados." (Microsoft, 2006:24).

2) Toma de decisiones. En este punto se evalúan los diferentes mecanismos de solución a los riesgos, pero se debe especificar cuál es el costo de cada recomendación a fin de tomar aquella que sea viable para la organización. Para poder tomar una decisión adecuada se consideran las siguientes actividades:
   - *Definición de requerimientos funcionales.* Se especifican las actividades, software, hardware, capacitación, etcétera necesarios para mitigar un riesgo.
   - *Selección posibles soluciones de control.* "Se elabora un listado de las diferentes alternativas de mitigación." (Microsoft, 2006:24).
   - *Analizar la solución.* "Evaluar los controles propuestos en contraste con los requerimientos funcionales" (Microsoft, 2006:24).
   - *Estimación de la reducción de riesgos.* Se debe analizar el nivel de riesgo que se mitigará, es decir en qué medida disminuye el nivel de exposición o la probabilidad de ocurrencia del incidente.
   - *Estimación del costo de la solución.* "Evaluar los costos directos e indirectos de la implementación de la solución." (Microsoft, 2006:24).
   - *Seleccionar la estrategia de mitigación.* "De acuerdo a un análisis costo beneficio se debe seleccionar la solución más efectiva y acorde a las necesidades del negocio." (Microsoft, 2006:24).
3) Implementación de controles. La implementación de controles implica la puesta en marcha de la estrategia seleccionada en la etapa anterior y para ello se definen dos actividades:

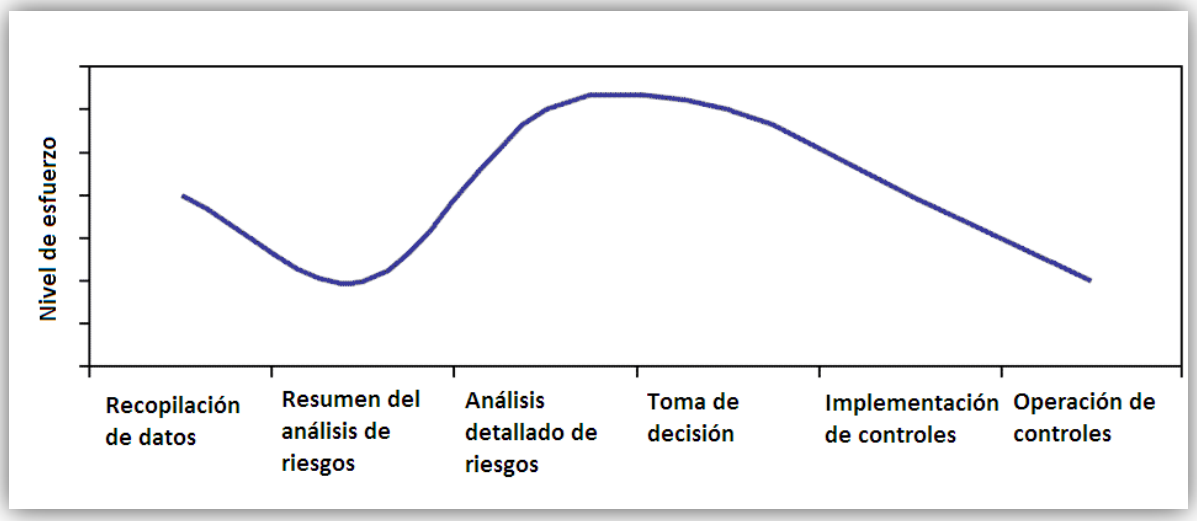
- *Realizar una implementación integral.* "La implementación debe involucrar tanto a las personas, procesos y tecnología." (Microsoft, 2006:24)
- *Organización por defensa en profundidad (defense-in-depth[1]).* Esta actividad involucra la aplicación de un control por nivel de protección.

4) Evaluación de la efectividad del programa. Es necesario ante una implementación mantener un control sobre las actividades ejecutadas para definir una estrategia de actualización o mejoramiento. Una herramienta que se puede emplear es el desarrollo de una "tarjeta de desempeño" donde se pueda incorporar la evolución de los procedimientos aplicados, por lo que es necesario establecer métricas para su evaluación.

En este mismo sentido Microsoft (2006) indica que cada etapa involucrará un nivel de esfuerzo distinto como se muestra en la gráfica siguiente:

[1] La estrategia *Defense-in-depth* es un conjunto de buenas prácticas para la aplicación de técnicas y tecnologías en la evaluación y mitigación del riesgo. Esta estrategia "recomienda mantener un balance entre las capacidades de protección, costos, rendimiento y consideraciones operativas." (NSA, *s.f.*) De tal forma que la conformación de la estrategia en profundidad involucra una acción definida para las personas, la tecnología y las operaciones.

Fig. 10 Nivel de esfuerzo de las fases de la gestión del riesgo



Fuente: Microsoft, 2006

Podemos observar que las etapas de mayor nivel de esfuerzo son las de Análisis detallado de Riesgos y la de Toma de decisión, de la primera es posible entenderlo debido al hecho que el análisis se realiza en cada proceso de tratamiento de la información de la empresa, además de los datos deben compararse con respecto a ejercicios anteriores o a estándares de la industria.

En cuanto a la toma de decisión se requiere de un alto esfuerzo de parte de la dirección empresarial pues se definirán estrategias que pueden afectar a la corporación en particular sobre cuál será el camino para resolver los problemas y las responsabilidades que se habrán de adquirir por área.

Debe destacarse que aunque técnicamente la implementación y operación de controles suelen requerir tiempo y recursos para su administración, los niveles de esfuerzo son menores dado que una vez definidos y aplicados a los procesos su operación es automatizada, lo que permite facilitar la tarea, liberar tiempo del personal y obtener información estratégica para otras áreas.

2.2. El Análisis de riesgos

En general, entre los modelos para la gestión del riesgo y administración de la seguridad de la información se define una etapa de análisis, la cual se convierte en el elemento clave para que la gestión tenga los efectos deseados. Ahora bien, por análisis de riesgos debe entenderse "el proceso cuantitativo o cualitativo que permite la evaluación de riesgos. Esto involucra una estimación de incertidumbre del riesgo y su impacto." (Del Carpio, 2006:104).

En general, el paso previo al análisis es la determinación de amenazas, siendo uno de los más importantes en el proceso, pues es aquí donde se genera una visualización de la situación de una organización con respecto a su brecha de seguridad y, en particular, podría mostrar la visión que tiene un delincuente informático de la empresa, así la pregunta a resolver en la fase de identificación es: "¿Cuales son todas las posibles amenazas a las que está expuesto un componente específico y que tan severas son?" (Microsoft, 2009)

En una primera aproximación, esta identificación se puede desarrollar a partir de análisis previos realizados en la empresa, sin embargo si es la primera vez que se realiza, algunos autores recomiendan la participación de un equipo especializado como podría ser una consultora que desarrolle una auditoría de seguridad. En otros casos podría ser posible a partir del uso de estadísticas mundiales o locales de los riesgos más frecuentes en la red. Lo importante es lograr una organización y clasificación que contrastaste con los tres principios fundamentales de la seguridad de la información (confidencialidad, integridad y disponibilidad) para alinear los riesgos a los procedimientos de la organización. Por ejemplo, una de las técnicas que nos sugiere Microsoft (2009) es el uso de las amenazas STRIDE[2] (por sus siglas en inglés), con las cuales se puede construir la siguiente tabla de alineación de riesgos y los principios de seguridad:

[2] STRIDE. Por sus siglas en inglés se refiere a las amenazas: ***S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service y **E**levation of privilege*

Tabla 1 Alineación de riesgos y principios de seguridad

Amenaza / Riesgo	Principio de seguridad	Significado	Ejemplo
Spoofing	Autenticación	Usurpar la identidad de algo o alguien	Pretender ser el director de la compañía o presentarse como alguien de una empresa.
Tampering	Integridad	Modificación de datos o códigos	Modificar un archivo en un disco o información a través de una red.
Repudio	No repudio	Negar una acción realizada	"Yo no envié el correo" "Yo no modifiqué la investigación"
Divulgación de información	Confidencialidad	Divulgar información a alguien no autorizado para conocerla	Publicación de los resultados de una investigación tecnológica o de un secreto industrial
Negación de servicio	Disponibilidad	Negar o degradar el servicio a alguien	Negar el acceso a la base de datos de la empresa a alguien que tiene autorización.
Elevación de privilegios	Autenticación	Obtener privilegios sin autorización	Que un usuario instale programas sin autorización

Fuente: Microsoft, 2009

Ahora bien, a partir de la identificación es posible realizar una evaluación cuantitativa o cualitativa de la exposición al riesgo y su impacto con respecto del negocio. Roberts (2001) indica que con frecuencia se elabora una valoración cualitativa antes que la cuantitativa, aunque no existe una razón para llevar a cabo un orden predefinido.

El análisis cualitativo de riesgos consiste en la elaboración de una tabla con valoraciones en tres niveles respecto de la amenaza a analizar: Alto, Medio y Bajo. En la mayoría de los casos la primera representación que se desarrolla es la Tabla de Probabilidad de Impacto. El significado de los niveles considerados es el siguiente:

- Alto: Muy Probable, se esperan dos o más impactos durante un año
- Medio: Probable, se espera algún impacto en dos o tres años
- Bajo: Poco probable, no se esperan impactos en menos de tres años

Nota: Esta clasificación propuesta de los niveles puede modificarse de acuerdo al nivel de madurez de seguridad que presente la empresa y a sus prioridades o cumplimientos regulatorios. De igual forma puede considerarse por periodo de tiempo o por número de transacciones de información.

La representación gráfica de la tabla se puede observar en la siguiente tabla:

Tabla 2 Probabilidad de impacto

Probabilidad / Riesgo	Alto	Medio	Bajo
Robo de información			
Usurpación de identidad			

Fuente: Microsoft, 2006

Otro de los aspectos a considerar para la toma de decisiones bajo un esquema cualitativo es a partir de una tabla construida con respecto al nivel de exposición que se tiene ante una vulnerabilidad o amenaza. En este caso los niveles se asocian al número de medidas implementadas para contrarrestar un riesgo, por ejemplo en una visión básica los niveles podrían indicar lo siguiente:

- Alto: Cuando no existe ningún mecanismo de protección
- Medio: Cuando existe algún mecanismo en el proceso

- Bajo: Cuando existe un mecanismo para cada etapa y riesgo

Tabla 3 Nivel de exposición al riesgo

Nivel de exposición / Riesgo	Alto	Medio	Bajo
Robo de información			
Usurpación de identidad			

Fuente: Microsoft, 2006

Tomando como base ambas tablas y considerando el impacto al negocio se puede construir la Tabla de Nivel Impacto, la cual indica que tan alto es el impacto al negocio ante la ocurrencia de un incidente de seguridad.

Tabla 4 Nivel de impacto

		Impacto al negocio		
Riesgo	**AI***	Impacto Moderado	Alto impacto	Alto impacto
	MI*	Bajo impacto	Impacto Moderado	Alto impacto
	BI*	Bajo impacto	Bajo impacto	Impacto Moderado
		Bajo	**Medio**	**Alto**
		Nivel de exposición		

Fuente: Microsoft, 2006

(*) Bajo Impacto, Mediano Impacto, Alto Impacto al negocio

En el caso del análisis cuantitativo del riesgo, se puede partir de las tablas anteriormente descritas pero asignando escalas de diferentes valores para cada nivel de exposición o probabilidad. Para ello debe establecerse la tabla que especifique el significado de los valores, por ejemplo:

Impacto * Probabilidad = Nivel de riesgo			
Rangos de impacto		*	**Rangos de probabilidad**
Alto	10 -- 7		10 – 7
Medio	6 -- 4		6 – 4
Bajo	3 -- 0		3 -- 0

La Tabla 4 bajo un análisis cuantitativo puede observarse de la siguiente manera:

Tabla 5 Nivel de impacto (Cuantitativo)

	A	10	0	10	20	30	40	50	60	70	80	90	100
		9	0	9	18	27	36	45	54	63	72	81	90
		8	0	8	16	24	32	40	48	56	64	72	80
		7	0	7	14	21	28	35	42	49	56	63	70
Impacto		6	0	6	12	18	24	30	36	42	48	54	60
	M	5	0	5	10	15	20	25	30	35	40	45	50
		4	0	4	8	12	16	20	24	28	32	36	40
		3	0	3	6	9	12	15	18	21	24	27	30
		2	0	2	4	6	8	10	12	14	16	18	20
	B	1	0	1	2	3	4	5	6	7	8	9	10
			0	1	2	3	4	5	6	7	8	9	10
			B					M					A
							Probabilidad						

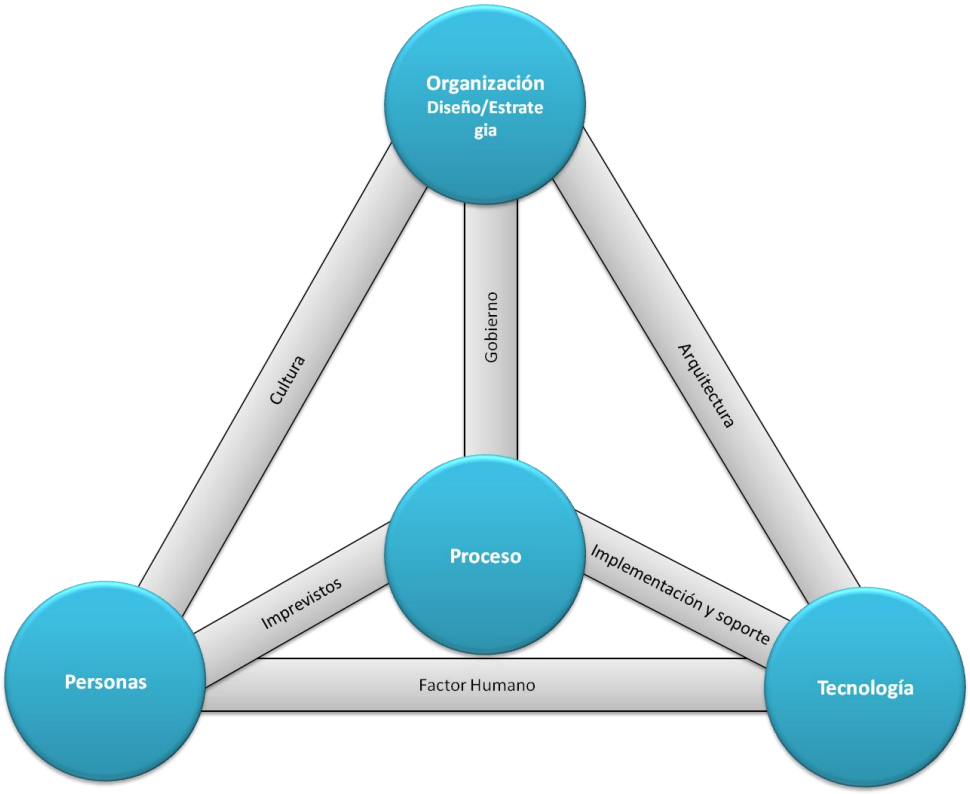
Fuente: Microsoft, 2006

Es importante aclarar que en algunos proyectos, solamente se puede ejecutar un análisis cualitativo. En especial porque la naturaleza del proyecto y la disponibilidad de tiempo y dinero influyen en el tipo de técnica a utilizar. Por lo general los proyectos grandes y complejos que involucran tecnología de punta requieren la aplicación de técnicas cuantitativas.

2.3. Gestión sistémica de la seguridad informática

En el año 2009 la Asociación para Sistemas de Auditoría y Control de Información (ISACA) publicó un documento titulado *Introducción al Modelo de Negocios para la Seguridad de la Información* con base en el trabajo presentado por Kiely y Benzel (2009) de la Universidad del Sur de California. En este documento se presenta una variante a los modelos tradicionales de seguridad y gestión del riesgo informático, pues por primera vez se presenta bajo un enfoque sistémico donde se establecen cuatro nodos relacionados con el desempeño de una organización (Organización, gente, proceso y tecnología), los cuales se encuentran unidos mediante diversas relaciones que representan diversos grados de riesgo entre los nodos, haciendo referencia a la protección de la información y de las identidades de los usuarios involucrados en el sistema. A continuación se muestra el modelo de gestión sistémica de la seguridad (Oliver, *et. al.*, 2009):

Fig. 11 Gestión sistémica de la seguridad informática



Fuente: Oliver y *et. al.* 2009

El diagrama anterior presentado por Oliver y *et. al.* (2009) y Kiely y Benzel (2009) tiene su principal aportación en la incorporación del nodo "proceso", pues tanto los modelos de seguridad como los de gestión de riesgos se basan principalmente en la interacción de los otros nodos teniendo como principal desventaja el hecho de que a pesar de que la información es importante, su propuesta de valor no se basa en los beneficios que aporte la gestión de riesgos en el proceso de negocio. La interpretación de este modelo debe analizarse tomando en cuenta que cualquier cambio en las relaciones o en los nodos tendrá una consecuencia en el equilibrio de la pirámide, es decir, el funcionamiento del sistema.

A partir de lo anterior se describe el significado de cada uno de los nodos y sus relaciones:

Nodos

- Organización. Este nodo se refiere a la importancia de los diseños y estrategias que implementa una empresa para alcanzar sus objetivos y a partir de esto generar ventajas competitivas. La definición de estrategias establece qué posición ocupará una estrategia de seguridad de la información en la empresa. En términos de seguridad de la información, el diseño corporativo puede establecer cómo se difunde la información a la organización y cómo se coordinan las diferentes áreas para la ejecución de los procesos de la empresa encontrando diferentes tipos de riesgo durante su flujo. Se destaca que de acuerdo a Kiely y Benzel (2009), problemas en el diseño de la estructura organizacional, la falta de planes relacionados con la toma de riesgos y el manejo de incentivos dentro las organizaciones se pueden observar en una productividad deficiente. Finalmente esta parte de la organización debe definir mecanismos de acción ante la presencia de riesgos a todos los niveles.

- Personas. A pesar de la gran evolución de las tecnologías en los últimos años el factor humano es indispensable para llevar a cabo las actividades de organización, siendo este mismo el eslabón más débil de la cadena de seguridad, pues acciones intencionales o accidentales efectuadas por el personal pueden comprometer el alcance de los objetivos organizacionales.

  En este modelo este nodo está representado no sólo por las personas que trabajan al interior de la compañía sino también por clientes y/o proveedores que están involucrados en algún proceso. Sin embargo es el personal interno donde se cuenta con mayor control para establecer mecanismos de seguridad, de tal forma que como lo menciona Kiely y Benzel (2009) este nodo debe partir de la descripción de puestos donde se evalúen niveles de riesgo y conocimientos relacionados, sin dejar atrás el proceso de reclutamiento que involucra la selección adecuada de los recursos humanos, la cual debe involucrar a los niveles jerárquicos necesarios.

  El último punto que se toma en cuenta en este nodo son las libertades civiles o derechos humanos que deben respetarse en todo momento ya sea en la descripción de puestos, la selección del personal o en las actividades a desarrollarse, en particular los derechos a la privacidad que en los últimos años han tenido gran relevancia en la sociedad.
- Tecnología. Actualmente la tecnología se ha convertido en el motor fundamental para la colaboración y los procesos de negocio, sin embargo un mal diseño en la implementación y/o configuración de la tecnología puede abrir vulnerabilidades que comprometan la integridad de la información y la continuidad de los procesos de negocio. Por otro lado es la misma tecnología la que propone soluciones para problemas de confidencialidad de la información basada en el desarrollo y aplicación de sistemas para identificación y autorización de acceso a los datos. Es importante hacer notar que la aplicación de tecnología de seguridad debe

hacerse tanto de manera interna como de modo externo, tomando en cuenta tanto cuestiones de seguridad lógica como física.

- Proceso. El proceso es un nodo que depende fuertemente de la existencia de los demás pues un proceso no puede existir si no existe el recurso humano que lo lleve a cabo, una organización que requiera de su ejecución para alcanzar sus objetivos y la tecnología que procure los elementos necesarios para su ejecución. Para este modelo el proceso se refiere a un *proceso de seguridad*, es decir, el método que utiliza una empresa para implementar y alcanzar sus objetivos de seguridad. Este proceso involucra la determinación de riesgos, elaboración de una estrategia de seguridad, implementación de controles, evaluaciones y monitoreo y actualización.

Relaciones

- Factor humano. Bajo esta relación se conecta a las personas con la tecnología y cabe resaltar de este punto que la tecnología por sí misma no resuelve los problemas de seguridad de una organización. Bajo este nodo se presenta la problemática de que a pesar de que la tecnología esté alineada con los procesos de negocio, tome en cuenta situaciones culturales y la estructura organizacional no será tan eficiente si la tecnología no es fácil de administrar (Kiely y Benzel, 2009), pues el propósito de la tecnología debe ser facilitar los procesos de negocio y no dificultar su ejecución.

  De acuerdo a Majachrzak (2004) en esta relación existen cuatro riesgos: al compartir información, accesos no autorizados, omisiones en los procesos de seguridad e intrusiones físicas.

- Cultura. La cultura es el vínculo entre la gente y la organización, en este sentido debemos tomar en cuenta dos posiciones importantes: la cultura del personal, consecuencia del entorno donde se desarrolla el individuo, y la cultura organizacional que responde a prácticas, patrones de comportamiento y actitudes del personal dentro de la empresa. Es importante esta relación pues los patrones de comportamiento que tienen

los trabajadores dentro de la organización pueden convertirse en reglas y normas a cumplirse.

En este sentido existe una relación entre las normas preestablecidas en las políticas de la empresa, así como las que se llevan a cabo como práctica de la empresa, siendo un problema de seguridad cuando no existe congruencia entre políticas y prácticas. Así mismo la cultura puede influir en lo siguiente:

- ✓ Problemas estratégicos y de diseño
- ✓ Problemas de actitud
- ✓ Toma de decisiones
- ✓ Tráfico de influencias
- ✓ Innovación y creatividad

- Gobierno. En entorno de gobierno se considera tanto el gobierno corporativo como las políticas y regulaciones nacionales. En el primer caso, se debe tomar en cuenta la posición que ocupa la seguridad de la información en la estructura misma de la empresa resaltando el hecho de que si la seguridad no se observa de manera global en la estructura se limita su eje de acción quedando sólo en la responsabilidad de un grupo limitado de personas.

  No debemos olvidar que la cultura influye de manera directa en el desempeño de la organización y en este sentido sabemos que el liderazgo dentro de la organización puede llevar al éxito, es por ello que la labor de seguridad de la información debe plantearse desde los niveles directivos dentro de la empresa y es desde este punto donde deben surgir las políticas y estrategias, logrando así alinear cada una de las acciones de los trabajadores ante eventos de seguridad donde se obtenga un beneficio mutuo entre las áreas involucradas, fomentando así la confianza en la organización.
- Arquitectura. En el caso de seguridad, entendemos arquitectura como el conjunto de procedimientos, políticas, personas y tecnología que componen

las prácticas de seguridad de una compañía (Kiely y Benzel, 2009); mientras que para la seguridad de la información describe el diseño o estructura del sistema de seguridad que comprende conexiones, elementos de hardware y software y toda la infraestructura necesaria para el funcionamiento del entorno de tecnologías de información. Es por ello que esta es una de las áreas más exploradas en la gestión de riesgos pues de aquí se desprenden los elementos basados en tecnología que permiten proteger la información es sus diferentes formas, como puede ser el caso de los antivirus, los firewalls, entre otros dispositivos.

Lo interesante de esta relación es el hecho de que las políticas establecidas para permitir acceso a fuentes de información, así como para garantizar la integridad de la misma deben partir desde la estructura fundamental de empresa, logrando así que cada área aplique medidas de control de acuerdo a sus requerimientos.

- Implementación y soporte. Esta relación existe partiendo del hecho de que tanto la empresa como la tecnología evolucionan constantemente de tal forma que la implementación de nuevos elementos de infraestructura o procesos debe ser controlada y actualizada constantemente. Se debe observar también que esta labor debe permitirle a una organización no sólo soportar sus procesos mediante tecnología sino también a establecer sistemas flexibles que permitan al proceso crecer de acuerdo a nuevos requerimientos.
- Imprevistos. Esta relación identificada por Kiely y Benzel (2009) como "*emergence*" se refiere al conjunto de actividades o patrones que ocurren durante el funcionamiento de la empresa y que no podían ser previstos y que además no es posible predecir su comportamiento ni consecuencias. Lo importante a notar es que los procesos por sí mismos están diseñados para lograr un objetivo, sin embargo si se observa su funcionamiento de manera continua se pueden identificar oportunidades que podrían derivar en un riesgo a la organización, lo que representa una ventaja a la empresa al

anticiparse ante eventualidades, al mismo tiempo podría lograr nuevas prácticas dentro de sus procesos.

A partir de esto han surgido los programas de mejora continua en seguridad y medidas preventivas como los planes de continuidad de negocio o recuperación de desastres. Finalmente menciona Kiely y Benzel (2009) que volver parte de las prácticas de la organización el análisis continuo de estos eventos y la búsqueda de medidas para su prevención no sólo en términos de riesgo sino en todas las áreas, puede permitir a la organización innovar continuamente en sus procesos.

Durante este capítulo se han descrito diferentes modelos de gestión de la seguridad de la información y a pesar de que no se mencionan todos los modelos relacionados con la gestión, existe una gran diferencia entre los modelos propuestos, por una parte, por Sena y Tenzer (2009), Arbeláez (2008) y Microsoft (2006), y por la otra, la propuesta de Oliver y *et. al.* (2009) y Kiely y Benzel (2009), pues los primeros basan su análisis en la identificación de riesgos informáticos mientras que los segundos se enfocan en un análisis de la organización donde intervienen cada una de las partes involucradas en el tratamiento de la información incorporando el análisis de riesgos por cada una de las etapas. Como consecuencia es posible desarrollar una estrategia que de inicio compatibiliza los requerimientos de la empresa para el alcance de sus metas y los objetivos de seguridad necesarios para su operación.

Cabe destacar que el modelo propuesto por Kiely y Benzel (2009) es el primero que se desarrolla bajo un enfoque sistémico y que por lo mismo es susceptible de ser mejorado, en particular porque abre la discusión con respecto a temas de gobernabilidad a fin de que se puedan tener esquemas base para la implementación de políticas en empresas de todo tipo. Por su parte en el ámbito de los recursos humanos existen dos puntos a profundizar, el primero relacionado con el desarrollo de una cultura que esté basada en el uso de buenas prácticas de

seguridad para el manejo de los sistemas y la segunda en procesos de selección de personal que faciliten conocer las capacidades de los trabajadores para manejar situaciones de riesgo.

Uno de los principales elementos que hace falta desarrollar dentro de este enfoque es la definición de acciones claras a efectuar dentro de cada uno de los nodos que propone el autor, siendo este el punto clave que se discutirá en el siguiente capítulo con el objetivo de que un administrador de sistemas o seguridad tenga elementos mínimos a ejecutar para el desarrollo de su estrategia independientemente del tipo de sistemas que maneje como parte de su infraestructura.

Capítulo 3. Gestión de la seguridad de la información

Hasta el momento hemos revisado tanto los procesos para la gestión de la información como los diferentes modelos que permiten gestionar el riesgo informático. Es importante destacar que el modelo de Kiely y Benzel (2009), así como la propuesta de Oliver y *et. al.* (2009) simplemente describen las actividades que a su consideración deberían desarrollarse pero no especifican las diferentes maneras para llevarlo a cabo.

De tal forma que la propuesta que se presenta en este documento pretende facilitar la implementación de un sistema de gestión de seguridad de la información partiendo del modelo propuesto por Kiely y Benzel (2009) mediante el establecimiento de acciones mínimas para los nodos de Organización, Tecnología, Recurso Humano y Proceso. Se ha partido del modelo de Kiely y Benzel (2009) debido a que su estructura facilita la alineación de los objetivos de seguridad con los organizacionales.

Como resultado se espera que a partir de su implementación, la seguridad de la información se establezca como parte del proceso de negocio que alcance niveles satisfactorios de protección a los procesos.

A pesar de que el modelo de Kiely y Benzel no indica en donde deben iniciar las acciones para la gestión de la seguridad de la información, la propuesta de esta tesis partirá inicialmente del nodo Organización pues es el que representa la definición de la estrategia de la corporación con respecto de todas actividades de la empresa. Posteriormente analizaremos el nodo Proceso que define a un proceso genérico donde es necesario aplicar mecanismos de seguridad de la información. En esta secuencia continuaremos con el análisis del nodo Tecnología que considera la implementación de herramientas para la gestión de información y finalmente analizaremos el nodo Recurso Humano, partiendo del hecho que es el último eslabón en la cadena de seguridad y se puede considerar que es el último que interviene en la gestión de seguridad.

3.1. Organización

Afirma Espinoza (2007:2) que el "desempeño sobresaliente de la seguridad es el resultado de estrategias múltiples diseñadas y aplicadas alrededor de un amplio espectro de temas y factores de riesgo dentro de una organización."

En general existen dos posturas al momento de desarrollar estrategias corporativas entorno a la seguridad de la información. La primera de ellas basada en los medios para proteger la información y la segunda priorizando la seguridad de la información como un fin.

Cuando nos referimos a la primera perspectiva encontramos que a pesar de que en el mercado existen un sinnúmero de herramientas, éstas tienden a fallar al dejar fuera de contexto a las personas y los procesos organizacionales quedando su aplicación en un entorno sumamente limitado. La principal consecuencia de este hecho para los administradores de seguridad es una modificación constante en sus estrategias debido al rápido surgimiento de innovaciones tecnológicas de seguridad e incrementando los costos debido a nuevas adquisiciones. Al respecto menciona Cano (2010) que los elementos técnicos representan sólo una parte de la seguridad de la información y que tarde o temprano un administrador deberá establecer acciones que involucren al personal, a los procesos y a los clientes y proveedores.

En la otra perspectiva la seguridad se establece como un fin incorporando las medidas de prevención en el contexto donde se desarrollan las personas o los procesos organizacionales. Bajo esta visión es posible seleccionar el conjunto de herramientas que se adaptan a la realidad que vive una organización y que al mismo tiempo le permite visualizar su situación y requerimientos a futuro basados en el conocimiento mismo del negocio en todas sus áreas.

En particular el desarrollo de estrategias corporativas para el caso de la seguridad están basadas en los planes de continuidad de negocio y recuperación de desastres. Un plan de continuidad de negocio tiene como principal objetivo

garantizar la operación de las actividades críticas de la organización minimizando los impactos de una contingencia (Barbecho y Montero, 2009) y no sólo considera cuestiones técnicas sino también a los recursos humanos. Este mismo plan indica qué hacer cuando una contingencia se presenta y puede evaluarse mediante simulacros, *checklists* o una prueba de recorrido.

Un simulacro tendrá la ventaja de conocer la rapidez de acción con la que la empresa atiende un incidente de seguridad, las pérdidas económicas asociadas al tiempo de respuesta e identificará si los procesos establecidos responden a las situaciones presentadas. Desafortunadamente para realizar una prueba de simulacro es necesario contar con la infraestructura necesaria para llevar a cabo la evaluación sin afectar el funcionamiento del negocio.

En cuanto al uso de *checklists* se puede partir por las definidas en los estándares ISO/IEC 270001, ITIL o COBIT que establecen puntos mínimos de administración empresarial y de aplicación de elementos técnicos, sin embargo lo más recomendable es realizar listas propias a partir de las políticas de seguridad de la empresa pues por una parte están diseñadas para el contexto en el cual se desempeña una empresa y desde otra perspectiva permitirá analizar su pleno cumplimiento. En este caso su aplicación no requiere del uso de infraestructura adicional y puede realizarse en cualquier momento a diferencia de las pruebas de simulacro, aunque desafortunadamente no permite identificar situaciones que la política no contemple.

Dado que una prueba de recorrido analiza el proceso al tiempo que verifica los controles aplicados permite identificar cambios en los procesos que pudieran haber sido ignorados en las políticas. Estas pruebas requieren de un mayor nivel de esfuerzo que las *checklists* debido a que deben analizar el proceso y no sólo verificar controles.

Por su parte los planes de recuperación de desastres establecen una metodología que indica los pasos a realizar una vez que ha finalizado la

contingencia e involucran la elaboración de inventarios, reportes de pérdidas y medidas de prevención.

La elaboración de inventarios es importante porque define la situación actual de la empresa en cuanto a qué equipos de cómputo, bases de datos y sistemas se encuentran en funcionamiento y cuáles han sido dañados. Esto mismo permite la elaboración de los reportes de pérdidas, necesarios para aplicar los procesos de recuperación. Finalmente en función de ambos documentos se pueden establecer medidas para prevenir que un incidente de seguridad ocurra nuevamente bajo las mismas condiciones.

Existen dos puntos de alta relevancia con respecto a este nodo, el primero se refiere a la organización de la empresa, básicamente a su estructura jerárquica, puesto que establece la base para el intercambio de información y puede constituir un elemento que facilite o dificulte la toma de decisiones y que al mismo tiempo sea una estructura lo suficientemente flexible para adaptarse a los cambios.

Una buena estructura de gobierno dentro la organización debe permitir la rápida identificación de las personas capaces de tomar decisiones (IBM, 2008) por lo que no se recomiendan estructuras jerárquicas de gran tamaño pues dificultarán acciones donde se requiere cierto grado de responsabilidad. En ciertas estructuras jerárquicas no está definida una autoridad para la toma de decisiones lo cual "no sólo resulta frustrante sino que también tiene un impacto directo negativo en la consecución de los objetivos deseados." (IBM, 2008:1).

Ahora bien en el caso de seguridad de la información la principal propuesta es el establecimiento de personal especializado en esta labor siendo dos las acciones a ejecutar:

1) Establecimiento del área de *Seguridad y Privacidad* encargada de lo siguiente:
    - Definir la política general para la protección de la información

- Establecer criterios para la clasificación de información
- Definir procedimientos para el aseguramiento de los datos
- Identificar y analizar los niveles de exposición al riesgo de la empresa
- Dar atención a incidentes de seguridad de la información
- Tomar una decisión con respecto a la existencia de riesgos: mitigación, transferencia o aceptación.

Una de las principales dudas que se genera a partir de este punto es el hecho de dónde debería colocarse el área de acuerdo a la estructura organizacional de la empresa pues al tener la capacidad de establecer políticas y tomar decisiones con respecto a los procesos de la empresa debería establecerse en lo que se conoce como nivel C (*Chief Level*).

2) Establecimiento de una política de gestión de la información: El hecho de que una organización cuente con una política bien definida sobre cómo se gestionan los datos desde su adquisición hasta su eliminación facilitará la protección de la información. Pues la tecnología asociada, así como las responsabilidades y acciones del personal se sujetarán a lo establecido en la política.

   Ahora bien, lo único que resta establecer es qué contenido mínimo debe tener una política para la gestión de información, el cual debería cumplir con lo siguiente:

   a. Establecer los mecanismos por los cuales se ha de obtener información para la empresa
   b. Definir los propósitos para los cuales será utilizada la información recopilada.
   c. Definir mecanismos de almacenamiento y redundancia para los datos
   d. Establecer periodos de vida para la información
   e. Definir la clasificación de información
   f. Establecer el caso para el uso de sistemas de cifrado

g. Establecer un canal de comunicación para casos en que la información esté en riesgo

En algunos países se han definido regulaciones que obligan a las empresas a desarrollar una política de privacidad que debe ser notificada a los clientes, proveedores y trabajadores de la empresa donde se establezca de inicio que el dueño de la información es el individuo y por lo tanto tiene derecho a consultar su información en cualquier momento y solicitar su rectificación, cancelación u oposición.

Es importante destacar que salvo la excepción mencionada, no es necesario que la política de gestión de información se establezca en un documento independiente, pues la política puede incorporarse dentro de las políticas o manuales de calidad y responsabilidad social de la empresa.

3.2. Proceso

El siguiente nodo a desarrollar es el nodo Proceso pues en este nodo se comienza con el análisis de riesgo para tomar decisiones respecto a cómo se gestionarán los aspectos que pongan en peligro a la información. Es muy importante antes de analizar cualquier proceso a proteger que éste se encuentre completamente alineado a los objetivos organizacionales.

La principal función de la seguridad de la información en este nodo es aportar los elementos necesarios para que los procesos de negocio se desarrollen de manera adecuada, es decir, que la seguridad aporte los elementos necesarios para su ejecución. Al respecto explica RSA (2008) que cuando se presenta una nueva propuesta la actitud de los responsables de seguridad debe responder a esta frase: "Esto es lo que podemos apoyar por parte de la seguridad, nosotros observamos algunos riesgos y esta es la propuesta para mitigarlos", indica David Kent, Vicepresidente de Seguridad de Genzyme: "*If you are doing your job, you shouldn' even sound like a security person. The business does not care how many*

cases you wrote. 'How are you helping me meet my business objectives?" (RSA, 2008:13)

Lograr este objetivo puede ser algo complejo sin embargo una aproximación para alcanzarlo es a partir del análisis de riesgos como si se tratara de un negocio donde los clientes estén representados por los usuarios y el objetivo como proveedores del servicio sea atender y resolver sus requerimientos.

Es en este punto donde deben de ser aplicadas metodologías de gestión de riesgos anteriormente descritas pues necesitamos establecer una base para tomar una decisión sobre qué riesgos deberán atenderse con prioridad para mitigarlos, cuales podrán transferirse y cuáles deberán aceptarse sin tomar una medida preventiva. Para ello debemos comenzar con la elaboración de la tabla de probabilidad y nivel de riesgo, en este caso y para clarificar el proceso de elaboración de dichas tablas desarrollaremos un ejemplo práctico partiendo del análisis de riesgos informáticos presente en una *call center* y finalizaremos con las consideraciones necesarias para la toma de decisiones.

Indica Arbeláez (2008) que antes de realizar cualquier análisis de riesgos o implementación de seguridad lo primero que se debe desarrollar es el entendimiento de la organización y sus procesos. Por lo cual describiremos a la empresa en cuestión:

Eventos Premier (EP) es una empresa que se dedica a la organización y ejecución de eventos corporativos, en particular desayunos y sesiones de capacitación de empresas de tecnología quienes invitan a sus clientes para participar con ellos. El proceso de negocios de EP para la ejecución de un evento corporativo es el siguiente:

Fig. 12 Proceso de negocios de Eventos Premier

Fuente: Elaboración propia

Es importante destacar que durante todo el proceso existe intercambio de información tanto de manera interna como de manera externa y que la información que se comparte es la siguiente:

1) Cotizaciones
2) Propuesta de negocio
3) Base de datos de invitados que incluye nombre, teléfono, dirección y correo electrónico
4) Base de datos de asistentes al evento que incluye los mismo datos

Normalmente esta información es intercambiada por correo electrónico entre la empresa contratante y Eventos Premier y de la misma forma con los empleados implicados en el proceso. En particular la información que más se intercambia son las bases de datos para el *call center* que es la instancia que realiza la invitación vía electrónica y telefónica a los clientes sugeridos por la empresa contratante.

Para esta empresa en particular los riesgos a los que se enfrenta son los siguientes:

- Robo de información
- Pérdida de información
- Daño en la información
- Presencia de códigos maliciosos

- Negación de servicio

Así que partiendo de la información anterior determinaremos la tabla de probabilidad, nivel de riesgo, para finalmente poder tomar la tabla de impacto al negocio y tomar una decisión al respecto.

Para establecer la tabla de probabilidad de impacto dado que será elaborada a partir del uso de un método cualitativo será indispensable elaborar el criterio para seleccionar el nivel alto, medio o bajo de cada uno de los peligros existentes. En este caso la empresa cuenta con una política bien definida para determinar la probabilidad de acuerdo a lo siguiente:

- Alto: Ocurrencia de 100 o más incidentes de seguridad por evento
- Medio: Ocurrencia de 50 a 99 incidentes de seguridad por evento
- Bajo: Ocurrencia de 0 a 49 incidentes de seguridad por evento

De las estadísticas de la empresa sabemos que por riesgo ocurren los siguientes incidentes por cada mil invitados durante la organización de un evento:

Riesgo	Número de incidentes por cada mil invitados
Robo de información	6
Pérdida de información	15
Daño en la información	45
Presencia de códigos maliciosos	1
Negación de servicio	75

Fuente: Elaboración propia

Para nuestro ejemplo la empresa Eventos Premier desarrollará un evento en el cual se invitarán a 12800 personas. Considerando el caso de robo de

información, la empresa cuenta con seis incidentes de seguridad por cada mil invitados por lo que se estimaría la ocurrencia de 76 incidentes de este tipo para todo el evento, el cual bajo las políticas definidas por la empresa corresponde a un nivel bajo de probabilidad pues cumple con la condición de situarse en la ocurrencia de 0 a 49 incidentes por evento. De esta forma la tabla de probabilidad quedaría de la siguiente manera:

Tabla 6 Probabilidad de impacto para Eventos Premier

Probabilidad / Riesgo	Alto	Medio	Bajo
Robo de información		X	
Pérdida de información	X		
Negación de servicio	X		
Códigos maliciosos			X
Daño en la información	X		

De la tabla anterior podemos observar que los incidentes con mayor probabilidad de ocurrencia de acuerdo a la política establecida corresponden a la pérdida y daño de información junto con la de negación de servicio. Mientras que robo de información y códigos maliciosos corresponden a una probabilidad media y baja de ocurrencia respectivamente.

El nivel de exposición esta determinado por el número de mecanismos implementados para contrarrestar un riesgo informático, en este caso la empresa ha utiliza los siguientes controles con respecto a cada una de las amenazas que ha identificado:

Riesgo	Controles Implementados	Total de controles
Robo de información	- Sistemas de prevención de intrusiones - Sistema para la administración	4

		de derechos de acceso - Cifrado de información - Manejo de identidades	
Pérdida de información	-	Sistemas automatizados de respaldo	1
Daño en la información	-	Sistemas de respaldo	1
Presencia de códigos maliciosos	-	Implementación de sistemas antivirus y antispyware - Administración centralizada de antivirus - Implementación de firewall - Análisis de códigos maliciosos en sitios web y correo electrónico	4
Negación de servicio			0

Es importante observar que en las amenazas de robo de información la empresa ya ha implementado diferentes controles sin embargo no ha logrado que este evento tenga una probabilidad de ocurrencia baja como ocurre en el caso de los códigos maliciosos.

Para elaborar la tabla de nivel de exposición, la empresa ha definido la siguiente política:

- Alto: Cuando no existe ningún mecanismo de protección
- Medio: Cuando existe algún mecanismo en el proceso
- Bajo: Cuando existe un mecanismo para cada etapa y riesgo

Si tomamos en cuenta que la empresa ha implementado cuatro controles para robo de información, su nivel de exposición correspondiente sería Bajo de acuerdo a las políticas establecidas, mientras que para negación de servicio sería Alto dado que no se ha aplicado ningún control. A continuación se muestra la tabla de nivel de exposición para la empresa Eventos Premier:

Tabla 7 Nivel de exposición al riesgo para Eventos Premier

Nivel de exposición / Riesgo	Alto	Medio	Bajo
Robo de información			X
Pérdida de información		X	
Negación de servicio		X	
Códigos maliciosos			X
Daño de información	X		

Fuente: Elaboración propia

De la tabla anterior podemos observar que daño de información representa el nivel de riesgo más grande dentro de la empresa, pérdida de información y negación de servicio un nivel medio y robo de información y códigos maliciosos el nivel más bajo. Asimismo se puede observar que daño y códigos maliciosos coinciden con los niveles de probabilidad de la tabla 6, mientras que los otros riesgos tienen una posición diferente es por ello que debe realizarse una tabla que permita balancear entre la probabilidad y los niveles de riesgo.

Para ello haremos uso de la tabla 4 del capítulo 2, misma que colocamos a continuación:

		Impacto al negocio		
Riesgo	**AI***	Impacto Moderado	Alto impacto	Alto impacto
	MI*	Bajo impacto	Impacto Moderado	Alto impacto

	BI*	Bajo impacto	Bajo impacto	Impacto Moderado
		Bajo	**Medio**	**Alto**
		Nivel de exposición		

* Bajo Impacto (BI), Medio Impacto (MI), Alto Impacto (AI)

Así que tomando la información de las tablas de nivel y probabilidad de riesgo anteriores y la tabla de impacto podemos generar la tabla de Nivel de Impacto para Eventos Premier. Nuevamente ocuparemos como ejemplo el robo de información, el cual por probabilidad contaba con un valor Medio y en cuanto a nivel de exposición con un valor Bajo, por lo que al hacer el cruce de riesgo medio con bajo nivel de exposición obtenemos un bajo impacto en el negocio. La tabla completa quedaría conformada de la siguiente manera:

Tabla 8 Nivel de impacto para Eventos Premier

Impacto al negocio / Riesgo	Alto	Medio	Bajo
Robo de información			X
Pérdida de información	X		
Negación de servicio	X		
Códigos maliciosos			X
Daño de información	X		

Fuente: Elaboración propia

De la tabla anterior observamos que robo, pérdida y daño de información cuentan con el nivel de impacto más alto y que el robo y daño conservan un nivel bajo. A partir de esta información podríamos priorizar aquellas actividades de alto impacto al negocio, pudiendo por el momento aceptar los riesgos básicos.

Sin embargo tenemos tres actividades que suponen alto impacto para el negocio y deberán ser mitigadas, en este sentido debemos de tomar una decisión para saber con cual debemos trabajar en primera instancia. Para ello conformaremos una nueva tabla donde compararemos el impacto económico que genera cada uno de los riesgos.

Para ello lo primero que debemos analizar es cómo se calcula el costo de un incidente de seguridad informática, el cual se obtiene a partir del costo que genera la ocurrencia del evento (costo de un incidente, CI). Normalmente este valor no se puede determinar con exactitud si el evento no ha ocurrido con anterioridad en la empresa, sin embargo puede considerarse la siguiente fórmula propuesta por Microsoft (2009):

$$CI = Cp + Cl + Cla + Ct + Cr + Og$$

Donde:

- Cp: Costos debidos a la pérdida de la ventaja competitiva por la divulgación de información confidencial o de propietario.
- Cl: Costos legales.
- Cla: Costos laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
- Ct: Costos relacionados con el tiempo de inactividad del sistema (por ejemplo, productividad de los empleados perdida, ventas perdidas, sustitución del hardware, del software y de otras propiedades).
- Cr: Costos relacionados con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
- Og: Otros daños derivados, como la pérdida de la reputación o de la confianza del cliente.

En este caso asumiremos que la empresa cuenta con estadísticas de costos relacionados con incidentes de seguridad para cada uno de los riesgos mencionados, siendo estos los resultados.

Riesgo	Costo promedio del incidente
Robo de información	$2,000
Pérdida de información	$1,800
Daño en la información	$450
Presencia de códigos maliciosos	$3,000
Negación de servicio	$4,000

Fuente: Elaboración propia

A partir de estos datos y considerando la tabla de incidentes por cada mil datos y del número de empleados, podemos calcular el costo estimado del total de los incidentes que en promedio se esperan para este evento. Por ejemplo para el caso de pérdida de información se tienen 15 incidentes por cada mil datos, en total 192 incidentes considerando los 12800 datos (15*12.8), si tomamos este valor y lo multiplicamos por el costo unitario de la ocurrencia de pérdida de la información obtenemos un costo total de $345,600. De la misma manera se calcularon los datos de negación de servicio y daño a la información encontrando los siguientes resultados:

Amenaza	Costo total estimado de los incidentes
Pérdida de información	$345,600
Negación de	$3, 840,000

servicio	
Daño de información	$259,200

Fuente: Elaboración propia

En este caso para la empresa Eventos Premier será prioritario dar solución al conjunto de problemas que puedan derivar en una negación de servicio. En general los incidentes de negación de servicio son los primeros en ser atendidos por una empresa pues su costo en caso de ocurrencia suele poner en riesgo la continuidad y en consecuencia la operación de la organización.

Algo que hace falta determinar es el comportamiento de una organización en caso de que dos o más incidentes tengan un costo equivalente y que no sea tan claro qué problema de seguridad se deberá atender con prioridad. En este caso el último factor que debe considerarse es el costo de la implementación de una solución de seguridad (CIS), la cual puede calcularse a partir de la siguiente fórmula:

$$CIS = CT_{Hw} + CT_{Sw} + CC$$

Donde:

- CT_{Hw}: Costo total del harware
- CT_{Sw}: Costo total del software
- CC: Costo total de la capacitación

Finalmente es necesario que toda organización que realiza un análisis de riesgos, previamente evalúe la ejecución de los procesos a fin de detectar cualquier cambio o situación de riesgo que no sea evidente.

3.3. Tecnología

En el caso de la Tecnología se deben observar cuatro puntos en particular:

- Capacidad de integración de las herramientas: Esto significa que las herramientas deben de ser independientes del fabricante y deben de ser capaces de interactuar y respetar los niveles predeterminados de seguridad establecidos por otras aplicaciones o sistemas.
- Control de la información de manera centralizada: Esto debe permitir a los sistemas imponer políticas desde un solo equipo a toda su infraestructura de red.
- La capacidad de ofrecer control desde cualquier punto o tipo de dispositivo: A pesar de que el sistema esté centralizado debe de tener la capacidad cualquier usuario de poder acceder a su información desde cualquier punto, aún desde el exterior de la empresa siempre que la política así lo permita.
- Capacidad de establecer auditorías: En sistemas de seguridad se entiende por auditorías al registro de acceso, creación y modificación de los datos asignados. Esto puede permitir que en caso de incidentes de seguridad se conozca qué usuario y en qué momento realizó una acción determinada.

Ahora bien es importante que una empresa identifique los diferentes tipos de tecnología existentes para el manejo de la seguridad de la información:

a) Sistemas para el manejo de usuarios y equipos: Estos sistemas se basan en el establecimiento de un directorio centralizado normalmente conocido como Directorio Activo (Active Directory para los sistemas Windows y Ldap para los sistemas basados en Unix). Este sistema permite la asignación de roles a diversos usuarios y que administrado de la manera adecuada puede permitir una implementación técnica de las políticas empresariales, así mismo puede establecer roles de los diversos usuarios y con ello los permisos a los cuales tienen derechos. Por ejemplo, un sistema de este tipo

puede asegurar que un usuario almacene información siempre en la misma carpeta, facilitando al administrador la creación de respaldos.

b) Sistemas para el manejo de identidades: Estos sistemas consisten en que a partir de la creación de un usuario en un sistema de cómputo se pueda una identidades que le permita acceder a diferentes servicios, es decir darle un rol dentro del sistema. La principal característica es que con la creación única de una cuenta se activará el usuario en los diferentes sistemas existentes en la red, a diferencia de un directorio activo que sólo existiría el usuario en esa clasificación y habría que crear uno diferente para cada subsistema existente.
c) Sistemas para la gestión de derechos de información. Estos sistemas permiten establecer permisos a documentos o carpetas en particular, de tal forma que un usuario puede decidir qué permisos dará a otros usuarios sobre sus documentos, por ejemplo pensemos que emitimos un documento confidencial que cuyo contenido puede ser conocido por dos personas, el dueño del documento puede establecer estas restricciones y de hecho puede proteger el documento contra escritura, impresión, envío de correo electrónico o copia a dispositivos extraíbles como memorias USB, CD 's, entre otros.
d) Sistemas de detección de intrusiones. Estos sistemas se ocupan para detectar patrones anormales o de completa intrusión a sistemas de cómputo, su principal ventaja en su aplicación es que permiten alertar a los administradores cuando alguien intenta ocasionar un daño intencional o no a los sistemas, al mismo tiempo que permiten establecer medidas de prevención automatizadas. Por ejemplo, el sistema detecta que dentro de su red existe una máquina que está enviando *spam* a los demás usuarios de la empresa, por lo que asume que la máquina está infectada y suspende su conexión de red al tiempo que alerta al administrador quien podrá analizar el equipo en búsqueda de códigos maliciosos o patrones de intrusión.

e) Sistemas para la generación de respaldos. Estos sistemas son muy importantes pues son los encargados de recuperar la información en caso de pérdida sin importar el motivo que lo ocasione. Para ello se basan en reglas para la generación de respaldos establecidos en periodicidad y tipos de contenido a respaldar.

3.4. Recursos humanos

A pesar de que se ha dejado al final este nodo, se debe notar que es el más importante dentro del proceso de gestión de la seguridad y probablemente el eslabón más débil de toda la cadena. Pues son las personas quienes operan los sistemas y finalmente quienes asignan o violan los permisos de la información.

En este sentido es fundamental para las empresas el desarrollo de campañas de concientización en materia de seguridad de la información, las cuales deben establecerse en todos ámbitos, es decir desde campañas basadas en información digital hasta la aplicación de cursos presenciales especializados en la material.

En este sentido una campaña de concientización debe constar de dos etapas fundamentales:

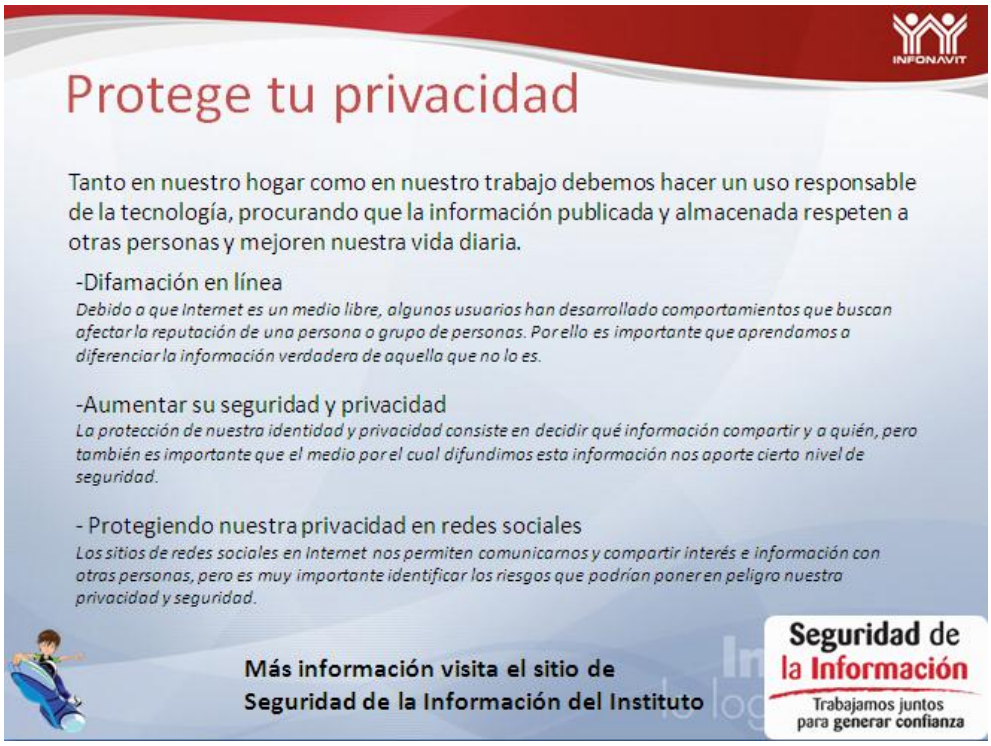
- Sensibilización: Esta primera etapa consiste en presentar a los empleados los diferentes riesgos que existen en Internet y en particular en su entorno de trabajo. Es muy importante que estos mensajes no fomenten miedo en la operación por lo que cada uno de ellos debe proponer soluciones a una problemática específica.

  Al día de hoy la empresa debe utilizar todos los medios disponibles para hacer llegar la información a sus empleados, por lo que se recomienda el desarrollo de boletines electrónicos de información los cuales pueden enviarse mediante correo electrónico a todos los empleados, en este punto se debe destacar que la campaña debe ser permanente y constante por lo que se deberá definir una fecha y horario para el envío de la información.

También puede complementarse con la impresión de folletos informativos acerca de las políticas establecidas en la empresa. La intención es aportar toda la información posible a los trabajadores, pero que sea de fácil interpretación.

La siguiente imagen corresponde al boletín informativo de la campaña de Seguridad de la Información implementada por el Instituto Nacional del Fondo para la Vivienda de los Trabajadores (Infonavit)

Fig. 13 Boletín informativo



- Acción: Esta etapa consiste en la implementación de acciones concretas y la invitación a los trabajadores a participar en los procesos de mejora de seguridad. Por ejemplo derivado del análisis de riesgos la empresa decide que es importante imponer un sistema para cambiar las contraseñas cada treinta días. En primer lugar la campaña de sensibilización deberá dar importancia al manejo seguro de contraseñas y por qué es importante

cambiarlas. En el momento que llegamos a la acción la empresa puede imponer un sistema de cómputo que obligue a los usuarios a realizar estos cambios.

En ambas etapas la empresa debe desarrollar mecanismos de evaluación de la propia campaña a fin de conocer qué información es de especial relevancia para los trabajadores y también para evaluar el éxito de la campaña.

Es para la empresa de suma importancia que implemente mecanismos, ya sea dentro de los contratos laborales o al momento de la entrega de la documentación relacionada con la descripción de la empresa que informe al trabajador de la existencia de políticas para la gestión de la información, así como de las sanciones relacionadas por el incumplimiento de dichas políticas.

Algo que no debe dejarse atrás cuando se trabaja con recursos humanos es la capacitación en la materia, debido a que la empresa podría invertir en sistemas de seguridad sin embargo si sus empleados no cuentan con la información necesaria para utilizarlos, de nada servirá la incorporación de nuevos sistemas y mecanismos.

Conclusiones y trabajo a futuro

La gestión de la seguridad de la información es un tema que se ha hecho más complejo derivado del desarrollo de las tecnologías de información y comunicaciones pero también de las distintas aplicaciones que las empresas y ciudadanos dan a la tecnología y de la cantidad de datos que se manejan.

Por lo mismo las estrategias de gestión de seguridad han ido evolucionando de acuerdo a la demanda del mercado pues durante los primeros ataques a las infraestructuras de cómputo a inicios los años 60 las empresas, que se enfrentaban principalmente a códigos maliciosos, llevaron a cabo inversiones millonarias en software y hardware especializado para detectar y eliminar este tipo de programas. Es en esta etapa que se desarrolla el mayor número de productos de seguridad: antivirus, firewalls, sistemas de prevención y detección de intrusiones, filtrados de contenido, mecanismos de acceso basados en *switches* y *routers,* entre otros.

Sin embargo su implementación no solucionó los problemas de seguridad en su totalidad y aunque estamos conscientes que en informática hablar de seguridad absoluta no es posible, ciertamente se puede tener niveles bajos de riesgo que permitan una operación óptima de los procesos de una organización. Es así que a partir de finales de los noventa y como respuesta a las nuevas tendencias de ataques se comienza a desarrollar modelos para la gestión de la seguridad de la información como un proceso administrativo e independiente de la tecnología, estándares como ITIL o la BS 17799 fueron los primeros en proponer una estructura para la gestión de las tecnologías de la información que facilitara el tratamiento de datos y que permitiera establecer controles para su uso. Abriendo el camino para el desarrollo de especialidades como el análisis del riesgo informático, los planes de contingencia y continuidad o el análisis de cómputo forense.

Uno de los retos más importantes al día de hoy es lograr establecer una estrategia de seguridad que esté completamente alineada con los objetivos empresariales y que responda a las solicitudes de los clientes o a regulaciones establecidas por los gobiernos para el manejo de los datos.

Así la principal conclusión de este trabajo es que antes de desarrollar una estrategia de seguridad es necesario conocer los procesos de la organización y el flujo completo de los datos. Es por ello que se partió de la descripción de la gestión de la información mediante la elaboración de dos modelos que representan las operaciones principales que se desarrollan en la empresa. Se recomienda profundizar en el tema pues existen algunas representaciones que describen un mayor número de etapas y responsabilidades por parte del administrador de los datos.

Partiendo de lo anterior y haciendo uso del modelo propuesto por Kiely y Benzel (2009) se sugieren acciones para las empresas que deseen implementar mecanismos para minimizar los riesgos informáticos, partiendo del hecho de que este modelo es la base para lograr los objetivos de seguridad con los corporativos a fin de que se convierta en una herramienta que genere beneficios.

De este modo en el nodo organización del modelo propuesto por Kiely y Benzel (2009) se sugiere la aplicación de políticas para el manejo de la información y la creación de un área de seguridad en la estructura orgánica en la empresa, como trabajo a futuro se sugiere seguir las discusiones acerca de cuál es la posición que debe ocupar la seguridad y la pertinencia de la existencia de áreas separadas para la administración de la información, la seguridad y los datos personales. Por su parte en el nodo personas se sugiere el desarrollo de campañas de concientización, un tema en el cual se debe profundizar pues la estrategia debe lograr un cambio de cultura en el manejo de las tecnologías. En cuanto al ámbito de la tecnología ya existe bibliografía especializada que describe los elementos

básicos de seguridad pero se recomienda estar al pendiente del desarrollo de nuevas tecnologías de protección o nuevas tendencias de ataque.

En cuanto al proceso concluimos que la gestión es diferente para cada tipo de empresa, ya sea por su tamaño o sector en el que se desenvuelve. Las acciones propuestas en esta parte del trabajo responden a requerimientos generales y deben de ser evaluados al momento de implementarse y complementados por otras medidas que el encargado de la seguridad considere. En este mismo punto sugerimos desarrollar guías o manuales dirigidos a sectores definidos, en particular a las empresas pequeñas y medianas quienes no necesariamente deben desarrollar un proceso de análisis de riesgos tan complejo como el presentado en el capítulo 3 pero que muchos de sus problemas podrían solucionarse con un diseño adecuado de políticas de uso de equipos e información.

Uno de los puntos que menciona Arbeláez (2008) es que la gestión de la seguridad debe desarrollarse como un proceso de mejora continua dentro de la organización por lo que se propone para otros trabajos el desarrollo de un sistema de indicadores y métricas que permitan conocer la situación actual de una empresa y la eficiencia de los programas de seguridad implementados. Este sistema puede apoyarse en las estadísticas que generan los sistemas de software y hardware. Otra alternativa es evaluar los modelos de madurez de seguridad la información que muestran una fotografía de cuál es la situación actual de una organización con respecto al objetivo que se ha planteado. En ambos casos también se requiere de un trabajo a fondo sobre la industria mexicana para desarrollar estudios que permitan conocer la adopción de estándares y dispositivos de seguridad en las empresas a fin de que en el mediano plazo se pueda establecer un criterio de evaluación estándar que determine la situación de México con respecto a otros países.

Entre las principales experiencias que hemos observado durante el desarrollo del presente documento es la velocidad con las que las tecnologías de

información y comunicaciones evolucionan, pues cuando se inició este trabajo a finales de 2008 los delitos informáticos representaban pérdidas a las organizaciones por 264 millones de dólares y fueron duplicadas en 2009 generando una situación más preocupante acerca de los riesgos derivados de la tecnología y que ha acelerado en algunos países el desarrollo de políticas públicas para la protección de la información.

Uno de los aspectos que ha evolucionado durante el desarrollo de este trabajo es el cómputo en la nube, una tecnología que busca que las empresas y usuarios utilicen el potencial de los servidores de Internet para administrar sus aplicaciones e información con el objetivo de ahorrar costos. Esta tecnología ha tomado gran auge cuestionando la validez del modelo propuesto en el capítulo 3 y que es necesario revisar puesto que el cómputo en la nube presenta nuevos retos en cuanto a la seguridad de la información y a pesar de que esta tesis se basa en un modelo sistémico de la seguridad de la información, en ningún momento se ha considerado que dentro del sistema existan elementos externos que intervengan directamente en la custodia y tratamiento de los datos.

Por lo que queda abierta la posibilidad a que el modelo sea modificado para incorporar otros nodos o relaciones que solucionen estas deficiencias. Pues tan sólo el análisis del flujo completo de los datos se verá afectado como consecuencia de que la información está distribuida a lo largo de Internet y de la empresa.

Finalmente para el Centro de Investigaciones Económicas Administrativas y Sociales se recomienda desarrollar un análisis a fondo de los elementos de innovación a nivel de hardware y software a fin de determinar una tendencia con respecto al uso de estas tecnologías y su aplicación en las empresas nacionales.

Por otro lado se sugiere realizar un análisis de los impactos de las nuevas políticas públicas derivadas de los retos que presenta la protección de datos. En particular nos referimos a la recién publicada Ley Federal de Protección de Datos Personales en Posesión de Particulares y los reglamentos derivados de la misma,

pues las actuales discusiones en la materia aseguran que se fomentará el desarrollo de las tecnologías en la empresa pequeña y mediana lo que sumado a políticas de apoyo para la automatización de este tipo de empresas se espera que tengan un efecto positivo en la economía nacional.

Bibliografía

Arbeláez, Roberto (2008). "Seguridad de información. Nuevos Retos para el sector público". En: *Semana de la Seguridad Microsoft 2008*, septiembre de 2008 Microsoft México.

Barbecho, Liliana; Montero, Andrea (2009). *Análisis del plan de continuidad negocio para una entidad bancaria, en el área de crédito y riesgo integral para el producto comercial factoring para el año 2009.* Guayaquil, Ecuador. Instituto de Universidad Superior Politécnica del Litoral.

Bennett, Todd (2000). *Distributed Denial of Service Attacks* [en línea]. Recuperado el 20 de octubre de 2009 de http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-whitepaper.html

Bianco, Carlos; Lugones, Gustavo; Peirano, Fernando; Salazar, Mónica (2002). "Indicadores de la sociedad del conocimiento e indicadores de innovación. Vinculaciones e implicancias conceptuales y metodológicas". En: *Seminario Internacional Redes, TIC's y Desarrollo de Políticas Públicas*. UNGS-EGIDA Firenze. Buenos Aires, Argentina.

Brown, Richard (2006). *Information security means better business* [en línea]. Computer Weekly. Recuperado el 20 de mayo de 2010 de http://www.computerweekly.com/Articles/2006/10/31/219436/Information-security-means-better-business.htm

Cano, Jeimy (2004). *Apuntes sobre la inversión y gestión de la seguridad informática* [en línea].Recuperado el 10 de septiembre de 2009 de http://www.virusprot.com/Art49.html

Cano, Jeimy (2009). *Seguridad de la información en Latinoamérica. Tendencias 2009*. Revista Acis Vol. 101. Asociación Colombiana de Ingenieros de Sistemas. Colombia

Casey, Eoghan. (2000) *Digital Evidence and Computer Crime.* Academic Press.

CERT (1997). *Denial of service attacks* [en línea]. Recuperado el 20 de octubre de 2009 de http://www.cert.org

Castro, Jose A. (2002). *La adecuada gestión del riesgo.* Revista SIC Número 52. Ediciones Coda/SIC

Cohen, Fred (1984). *Computer Viruses – Theory and Experiments*. Fred Cohen & Associates. Estados Unidos

CSA (2009). *Guía para la Seguridad en áreas de atención en Cloud Computing V2* [en línea]. Cloud Security Alliance. Recuperado el 20 de mayo de 2010 de http://www.cloudsecurityalliance.org/guidance/csaguide-es.v2.pdf

Del Carpio, Javier (2006). *Análisis del riesgo en la administración de proyectos de tecnología de información.* En: Revista Industrial Data, Vol. 9, Núm. 1. Lima, Perú.

Deloitte (2009). *Losing Ground – 2009 TMT Globas Security Survey*. Amstelveen, Holanda.

Deloitte (2010). *Ley Federal de Protección de Datos Personales en Posesión de Particulares.* En: Desayuno de Socios AMIPCI, agosto de 2010. México, Distrito Federal.

Ernst&Young (2009). *Outpacing Change – 12th Global Information Securtity Survey*. Estados Unidos

Espinoza, Carmen (2005). *Estrategia Organizacional: Alineando las herramientas de Gestión Humana en el desarrollo de una cultura de seguridad y prevención competitiva.* Biblioteca Virtual de Desarrollo Sostenible. Lima, Perú.

FTC. *El robo de identidad* [en línea]. Federal Trade Comission. Recuperado el 20 de octubre de 2009 de http://www.ftc.gov/bcp/edu/microsites/idtheft/en-espanol/index.html

Holton, Glyn (2004). "Defining Risk". Financial Analyst Journal Vol. 60 Núm. 6. CFA Institute.

IBM (2008). *Gobierno de TI: Obtener el máximo rendimiento en los momentos críticos* [en línea]. Recuperado el 30 de abril de 2010 de https://www-935.ibm.com/services/es/cio/pdf/obtener-maximo-rendimiento-en-_momentos-criticos.pdf

IC3 (2009). *Internet Report Crime 2009*. Internet Crime Complaint Center. Estados Unidos.

ISO (2007). *Information Technology – Security techniques-Information security management systems* ISO/IEC 27000 – *Overview and vocabulary*. International Standard Organization . Estados Unidos

Kiely, Laree; Benzel, Terry (2009). *Systemic Security Management: A new conceptual framework for understanding, the issues, inviting dialogue and debate, and identifying future research needs*. Institute for Critical Information Infrastructure Protection (ICIIP). Marshal School of Business. Estados Unidos.

LFPDP (2010). *Ley Federal de Protección de Datos Personales en Posesión de Particulares.* Diario Oficial de la Federación. México

Majachrzak, A (2004). *Human Issues in Secure Cross- Collaborative Knowledge – A Conceptual Framework for Understanding Issues and Identifying Critical*, ICIIP White Papers. Estados Unidos

McKemmish, Rodney (1999). *What is forensic computing?*. Australian Institute of Criminology. Canberra, Australia

Microsoft (2006). *The Security Risk Management Guide*. Microsoft Corp. Estados Unidos

Microsoft (2009). *IT Infraestructure Threat Modeling Guide.* Microsoft Corp. Estados Unidos.

Morales, Estela (2004). *El uso de la información y la reflexión, condiciones para llegar a la universidad del conocimiento* [En línea]. Revista digital Infodiversidad, Vol. 7. Recuperado el 25 de diciembre de 2009 de http//www.redalyc.uaemex.mx/redalyc/pdf/277/2777107.pdf

Navega Protegido (2009). *Principales riesgos de seguridad en las organizaciones* [en línea]. Navega Protegido en Internet. Recuperado el 20 de mayo de 2009 de http://navegaprotegido.blogspot.com/2009/05/principales-riesgos-de-seguridad.html

Oliver, Derek; Allard Jean-Luc; Antonsson Elisabeth; Bahl Sanjay; Brotby, Krag; Dimitriadis, Christos; Gupta, Meenu; Ledesma, Cristina; Youssef, Ghassan (2009). *An introduction to the business model for information security*. Information Systems Audit and Control Association (ISACA). Estados Unidos

Páez, Iraset (*s.f.*). *Gestión de Inteligencia, aprendizaje tecnológico y modernización del trabajo informacional. Retos y Oportunidades.* Caracas: Universidad Simón Bolívar.Caracas, Venezuela.

Paoli, Antonio (1989). *Comunicación e Información*. Editorial Trillas. México

Parra, Jairo (2000). *Tratado de la Prueba Judicial*. Ed. Librería del Profesional. Bogotá, Colombia

Pressman, Roger (2002). *Ingeniería de Software: Un enfoque práctico*. McGrawHill, 5° Edición. Estados Unidos

Robbins, Judd (1998). *An explanation of Computer Forensics* [en línea]. Recuperado el 19 de septiembre de 2009 de http://knock-knock.com

Roberts, Barney (2001). *The benefits of Integrated Quantitative Risk Management.* En: 12° Simposio internacional del Consejo Internacional de Ingeniería de sistemas. Melbourne, Victoria. Australia.

RSA (2008). *The Time Is Now: Making Information Security Strategic To Business Innovation* [en línea]. Recuperado el 15 de abril de 2009 de http://www.rsa.com/innovation/docs/RSA_strategic-security-APR.06.08_wo_mountain_print.pdf

Saferstein, Richard (1998). *Criminalistics*. Prentice Hall. Estados Unidos

Sena, Leonardo; Tenzer, Simon (2004). *Introducción a Riesgo Informático* [en línea]. Facultad de Ciencias Económicas y de Administración, Universidad de la República. Uruguay. Recuperado el 15 de mayo de 2009 de http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

Téllez, Julio (2003). *Derecho Informático.* 3ª ed., Ed. Mac Graw Hill. México 514p.

UNAM-CERT (*s.f.*) *Diccionario de términos de seguridad informática* [en línea]. Recuperado el 20 de octubre de 2009 de http://www.seguridad.unam.mx/usuario-casero

Velasco, Cristos (2006). *El robo de identidad en Internet, uno de los fraudes con mayor incidencia* [en línea]. UNAM Revista Enter@te. Año 5, Número 45. Recuperado el 15 de mayo de 2010 de http://www.enterate.unam.mx/Articulos/2006/enero/robo.htm