ANÀLISIS DE RIESGO EN LOS SISTEMAS DE INFORMACIÒN

SANDRA PATRICIA BUSTOS GUTIERREZ

JOSÉ SÁNCHEZ VILLEGAS

Asesor

LUZ MERY GUEVARA CHACÓN

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

ESPECIALIZACIÓN EN CONTROL INTERNO

BOGOTÁ D.C.

2013

ANÀLISIS DE RIESGO EN LOS SISTEMAS DE INFORMACIÓN

LISTA DE FIGURAS

Decían los senadores y dueños del poder en la antigua Roma que quien tiene la información, tiene el poder; muchos de ellos utilizaban a sus criadas como rameras, estos las prestaban a los legionarios y miembros de comisiones gubernamentales, para a través de ellas conseguir información sobre las pretensiones de sus enemigos políticos, y cualquier otra de interés, esta actividad les ayudaba a mantenerse en el poder y estar más seguros en sus cargos (Ardebol, 2003)

A través de los años hemos visto evolucionar la tecnología y las comunicaciones; en el siglo XIX la Revolución Industrial y científica, con inventos como: la locomotora, el primer proyector cinematográfico. El siglo XX se puede considerar como la Segunda Guerra Científica o Revolución Técnica; allí se da inicio, a unos de los descubrimientos más importantes a nivel de comunicación, como fue el desarrollo, invención y masificación de los medios de comunicación a través del computador e internet. En ese sentido el siglo XXI se podría considerar como el de la revolución cibernética, con el nacimiento de las redes sociales (Montañés y Simón, 1999)

Uno de los autores más importes que realizó un gran aporte fue, Norbet Wiener padre y fundador de la cibernética o control de la comunicación; nos hereda su pensamiento, el cual trataba de una ciencia multidisciplinaria para el análisis de los procesos similares que se dan en los seres vivos y las máquinas, como son el control de la información y las comunicaciones; donde la información es el origen, el medio y el fin (Wiener, 1948)

A partir de estos avances y múltiples pensamientos que aportan al desarrollo tecnológico, nace el concepto de seguridad de la información, entendiéndose, como el conjunto de medidas preventivas de las organizaciones públicas y privadas y de los sistemas tecnológicos que permiten proteger y resguardar la información, manteniendo la confidencialidad, la integridad y la disponibilidad de la misma (Montañés y Simón, 1999)

Según el texto sacado de internet, publicado por IE Cátedra Española año 2010 “La Gestión de Riesgos en los Sistemas de Información tiene como objetivo sensibilizar a los directivos de las empresas u organizaciones sobre la necesidad cada vez más perentoria de gestionar el riesgo derivado del uso de sistemas de información, superando el tradicional enfoque basado exclusivamente en la tecnología”.

La necesidad de seguridad de la información es crucial en todas organizaciones; el ineludible beneficio del uso de los medios electrónicos, informáticos y telemáticos no pueden ocultar la preocupación y la vulnerabilidad de tomar medidas idóneas para asegurar la confidencialidad de la información tales

como: Internet, fax, correos electrónicos, video conferencias chat, explorador web y enseñanza asistida por el computador.

Dos acontecimientos en el siglo XX, han generado conciencia a las organizaciones de los riesgos que pueden presentar los sistemas informáticos; uno de ellos, es el llamado efecto 2000 o nuevo milenio, el cual consistió en un error de software del tiempo y fecha, lo que significaba una amenaza a los sistemas informáticos, pues los ordenadores anteriores al 2000 tenían programadores para cambiar la fecha y hora del año, pero éstos habían sido programados con los años que empezaban con los dígitos de 19, por tanto, a la llegada del 31 de diciembre de 1999 se temía el fin del mundo o un desastre económico. Otro evento importante, fue la caída de las torres gemelas o el llamado efecto 11.9, 11 de septiembre, en donde Estados Unidos presenta la mayor crisis económica en el mundo y la pérdida de información de las organizaciones fue invaluable e irrecuperable. El resultado de estos acontecimientos, fue una explosión de legislación para reglamentar la seguridad de la información a nivel mundial, ya que la información y los sistemas que la soportan constituyen un recurso valioso para las organizaciones públicas y privadas e incluso para propias personas (Cocho, 2003)

Lo que se quiere lograr con este ensayo es generar conciencia y realizar un análisis de riesgos de las posibles amenazas a las que se ven expuestos los sistemas de información en las organizaciones o en las personas, por no establecer políticas, estrategias normas y procedimientos, para salvaguardar la información de sus negocio, evitando que esta caiga en manos de sus competidores o que se vuelvan públicas de forma no autorizada, ocasionando pérdida de credibilidad, pérdida de sus negocios, demandas legales e incluso la quiebra.

En este sentido y adentrándonos ya en el tema gestionar y analizar los riesgos en los sistemas de información se deben seguir unos pasos específicos que ayudan a manejar la incertidumbre: primero que todo debemos saber que es un problema potencial, que puede ocurrir o no; segundo se debe evaluar la probabilidad de que ocurra y tercero estimar su impacto y establecer un plan de contingencia, en caso de que el riesgo se materialice (Bravo y Sánchez, 2009)

Casi todos los días utilizamos las palabras datos, información y sistema, por ello es necesario que comprendamos su significado en general y la importancia que tienen en las organizaciones. Datos se deriva del latín datum que significa hecho, el cual puede ser un número, una afirmación o una imagen. Los datos son la materia prima en la producción de información (Cocho, 2003)

Por otra parte, la información la constituyen los hechos o las conclusiones que tienen un significado dentro de las organizaciones mediante procesos o manipulación de datos. En este sentido los datos a diferencia de la información, rara vez son relevantes e importantes; para convertirse en información deben ser manejados o tratados mediante la formación de tablas, suma, resta, división, o cualquier otra operación, que permita comprender mejor una situación; a este se le conoce como un proceso porque permite no sólo manipulación de la información, sino que también produce información útil en la organización, es decir, que sea relevante, que se encuentre completa, que sea precisa, que sea actualizada continuamente y se materialice en un beneficio económico. Entonces, un sistema es una matriz de componentes que se alinean para alcanzar una meta común, o varias, aceptando entradas, procesándolas, y produciendo salidas de una manera organizada. Los sistemas son cerrados o abiertos, los cerrados son sistemas independientes no tienen conexión con otros, no ingresa información, y tampoco

genera información para otros sistemas, un ejemplo sencillo es la impresión de cheques, solo se pueden realizar cuando un empleado ingresa los datos mediante un teclado. Ahora bien, los sistemas abiertos son aquellos que interactúan y se comunican con otros sistemas, pueden ser los programas de contabilidad, que reciben información de módulos de cuentas por cobrar y cuentas por pagar y generan información a otras áreas funcionales de la organización. Daremos un ejemplo mediante la (Figura 1).

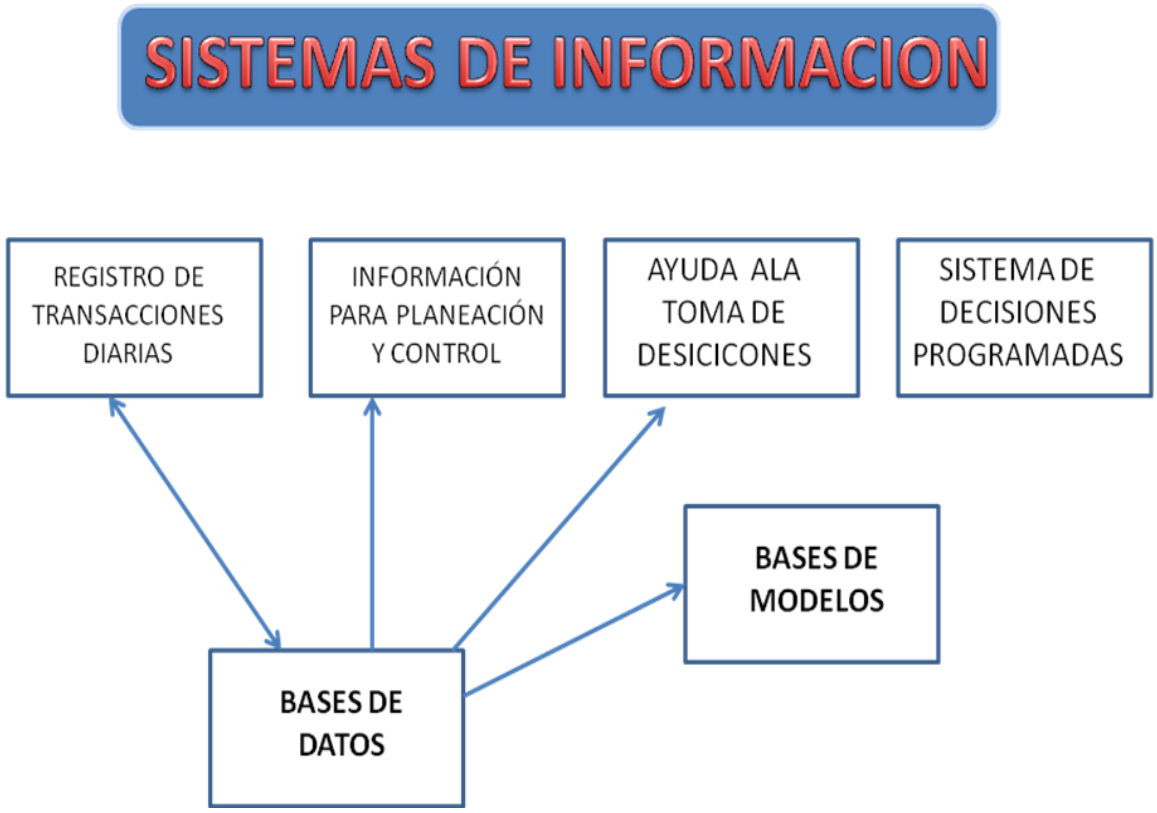
Figura 1.Generación de Información Entradas – Procesamiento- Salidas

Fuente: Effy oz, 2006 Administración de los sistemas de Información.

El concepto de sistemas de información, fundamentalmente consiste en un sistema integrado donde se desarrollan cuatro funciones principales: la primera, es el registro de transacciones u operaciones diarias de la empresa; la segunda, consiste en aportar información para planeación y control; la tercera es ayudar a la

toma de decisiones y la cuarta, tomar decisiones previamente programadas. (Figura 2).

Figura 2.Componentes del sistema de información (Montañés y simón, 1999)



Fuente: Montañés y Simón, 1999 Auditoría de los Sistemas de Información.

El primer componente corresponde a las entradas de un sistema de información, las cuales son provenientes de las transacciones efectuadas en el día a día de las organizaciones; puede ser, una venta, una compra, la contratación de un empleado nuevo, un pago efectuado a los proveedores; estas operaciones son

registradas en documentos y posteriormente, serán ingresadas a un sistema de computo, donde se consignaran a través de un sistema de procesamiento de datos o un sistema de registro de operaciones tales como: cajas registradoras, cajeros automáticos donde se realizan retiros, depósitos y transferencias; las salidas corresponden a la información para la planeación y control, producidas por los sistemas de información, generalmente el dispositivo utilizado con frecuencia, es el monitor o pantalla, aunque existen otros medios tales como: altavoces, dispositivos electrónicos que permitan la transmisión de esta información en forma codificada a otra computadora, para luego ser interpretada, permitiendo que esta sea una ayuda para la toma de decisiones; el cuarto componente contempla aquellos programas que ofrecen una decisión completa sobre un problema, conocidos como sistemas expertos, los cuales pretenden sustituir las funciones de los humanos en una área específica, así como tenerlas disponibles en cualquier punto donde se pueda ejecutar dicho programa (Effy Oz, 2006)

Los sistemas de información penetran todos los aspectos de nuestras vidas, los personales, mediante el acceso a redes sociales a través de la Web, tales como: facebook, skype, twitter, en los negocios se realiza mediante sistemas de administración de una cadena de suministros o sistemas de planeación de recursos empresariales (ERP) su sigla en Inglés (Enterprise Resource Planning), que corresponde a secuencia de actividades relacionadas con la generación de un producto o servicio; que proporcionan apoyo a los administradores para vigilar y modificar los procesos empresariales(Effy Oz, 2006)

En el mundo existen diferentes tipos de sistemas de información para funciones diversas dentro de las organizaciones, entre ellos están: los CRM (Administración de las Relaciones con los Clientes) Que por lo general ayudan desde la conservación de registros más sencillos de los clientes, hasta lo más

amplios análisis y hallazgos; podrían determinar cuando el cliente va a cambiarse a la competencia; quien utiliza estos sistemas podrá observar todo el historial del cliente con la empresa, lo que ha adquirido, las entregas que ha recibido, los pedidos no cumplidos y cualquier otra información que permita ayudar a resolver problemas que el cliente ha presentado con la organización; su objetivo principal es aumentar la calidad del servicio, reducir el recurso humano en la atención al cliente, y conocer lo más posible acerca de las preferencias de los clientes (Montañés y Simon,1999)

Existen también sistemas de inteligencia de negocios cuyo propósito es obtener relaciones y tendencias de los datos básicos que pueden ayudar a las organizaciones a competir mejor; son modelos estadísticos sostenidos, los cuales acceden a grandes cantidades de datos; por lo general corresponden a transacciones las cuales reposan en bases de datos; por otro lado están los sistemas para soporte de decisiones, los cuales corresponden a los desarrollos o diseños específicos dentro de las organizaciones para toma de decisiones. Se basan en modelos y fórmulas para producir tablas concisas o un número único que determine una decisión. (Derrien, 1994).

Los sistemas expertos son otro tipo de sistemas de información cuyo objetivo está basado en técnicas de inteligencia artificial, para soportar procesos de toma de decisiones que requieren muchos conocimientos; estos sistemas se programan para el procesamiento de datos, para efectuar comparativos; los sistemas expertos están conformados por una base de conocimientos, la cual contiene conocimiento modelado extraído del diálogo con un experto, adicionando una base de hechos o memoria de trabajo la cual recopila los hechos sobre un problema que se ha descubierto durante el análisis, sumándole el motor de Inferencia , el cual modela el proceso de razonamiento humano. Por otra parte

tenemos los modelos de justificación que tiene como finalidad explicar el razonamiento utilizado por el sistema para llegar a una determinada conclusión, por último se encuentra la Interfaz de usuarios, ya que es la interacción entre el Sistema Experto y el usuario (Effy Oz, 2006)

Cada vez son más las organizaciones que operan en todo el mundo, cada vez surge un nuevo negocio, empresa o proyecto, las cuales deben enfrentarse al desafío e implementación de sistemas de información, exponiéndose a una serie de riesgos que están presentes tanto a nivel externo, como a nivel interno: de carácter externo, se evidencian los riesgos del entorno, como factores de la economía, aspectos sociales, decisiones políticas, cambios en el mercado, estrategias de la competencia, cambios de la tecnología, y muchos otros que no le competen directamente a la empresa, negocio o proyecto, pero que si le pueden influir de una u otra forma. A nivel interno, los riesgos pueden ser más controlables, y van desde mal manejo de los recursos, falta de controles que expongan la empresa a robos y faltas a la ética, hasta pérdidas de diversos tipos por deficiencias en los controles (Ponce de León, 2002)

En la década de los 70's, en los países europeos, como consecuencia de la crisis petrolera, se obligó a muchos países limitados de este recurso a buscar alternativas amigables para su producción. Esta situación a su vez logra un impacto positivo en los países desarrollados, en la búsqueda de soluciones de los problemas más relevantes que pasaba el planeta en ese momento, entre ellos, cambios climáticos, crisis energética y la situación financiera; esta teoría se conoce hoy día como desarrollo sustentable, su objetivo principal, era la exigencia en el desarrollo de procesos productivos, que alcanzarán altos índices de efectividad y calidad e involucrando todos los campos de aplicabilidad (Scott, 1998)

Para un mayor entendimiento definamos análisis de riesgos, como un proceso de calidad o mejora continua que busca estimar las probabilidades de que se presenten acontecimientos indeseables, permitiendo medir la magnitud de dichos impactos negativos en el transcurso de ciertos intervalos específicos de tiempo. Lo que significa que no sólo es una observación detallada y sistemática, sino que es una propuesta metodológica que permite el conocimiento de los riesgos y sus fuentes o causas, las consecuencias potenciales y remanentes, y la probabilidad que esto se presente. Los principales tipos de riesgos que se pueden presentar en las organizaciones públicas o privadas y pueden ser: riesgos de la seguridad social y pública, los que involucran a un gran sector social y corresponden a los accidentes naturales o causados, generalmente graves y que ponen al borde la integridad humana, la frecuencia de este tipo de riegos tiende a aumentar e involucra cada vez más seguridad, la protección de vidas y materiales o productos. Algunos ejemplo son: Muertes, heridas, violaciones, robos, asaltos, daños en propiedades. También están los riesgos de higiene y salud: que se podrían entender como los efectos causados a la salud humana vegetal o animal, involucrando enfermedades continuas, crónicas o agudas; su tendencia es al aumento en impacto y frecuencia. Ejemplo: casos y tipos de enfermedades, niveles de mortalidad en la población, frecuencia y recurrencia de casos epidémicos; además los riesgos medioambientales, que son cambios causados en el entorno natural o laboral incluyendo los espacios públicos, produciendo efectos y alteraciones graves a la población y los ecosistemas, ejemplo: cambios de hábitat y ecosistemas, contaminación del agua, aire y suelo; los riesgos de Interés social: son aquellos que involucran las necesidades y las preocupaciones de comunidades y sociedades, en busca de nuevas costumbres. Ejemplo: restricciones en el uso de recursos naturales, aumento en el costo de servicios, convivencia social; finalmente los riesgos técnicos y de inversión son los que Indican la factibilidad y responsabilidad que están implícitos en cualquier intento de negocio, se consideran retos técnicos y financieros de las compañías u

organizaciones. Ejemplo: seguros, baja de tasas de interés, responsabilidades fiscales y pérdida del poder adquisitivo (Ponce de León, 2002)

Una vez identificados los riesgos en el entorno de la organización se deberá realizar la aplicación y utilización de instrumentos de análisis y evaluación de ellos, los cuales corresponden a pautas establecidas y lineamentos marcados por la gestión de la seguridad; estos deben tener unos pasos mínimos que cada organización adoptará y adaptará. Después de analizados los riesgos se debe establecer un equipo multidisciplinario de análisis, en donde un grupo de especialistas en cada uno de los campos que se tenga estimados para la realización del análisis de riesgo; establecido el equipo, se deben identificar los temas o parámetros de análisis: en esta etapa se debe de establecer los posibles riesgos a analizar y priorizarlos, para la identificación de recursos y puntos críticos que permitan establecer una estrategia conveniente para el mejoramiento continuo de los riesgos hallados en la organización; analizados e identificados los posibles riesgos se debe realizar la validación de resultados y se logra por medio de la presentación formal de los datos a los responsables de los departamentos y al nivel directivo y gerencial de la organización, los cuales poseen la capacidad y responsabilidad en la toma de decisiones; una vez clarificado la importancia de los análisis de riesgo, dentro de las organizaciones, podremos dar una conceptualización global de los sistemas de información y la importancia que representan dentro de los procesos productivos de las empresas (Ponce de León, 2002).

Por lo anterior es claro que las organizaciones deben enfrentarse con seriedad, a los riesgos y amenazas a los que están expuestos los sistemas de información basados en computadoras, ya sean naturales o por el hombre, lo cual no significa que no exista manera de salvaguardarla o asegurarla por completo

contra algún percance potencial; sin embargo, existe la manera de reducir de manera significativa los riesgos y recuperarse de las pérdidas; las metas que se tienen en cuanto al desarrollo, la implementación y el mantenimiento de los sistemas de información constituyen una parte grande y creciente del costo de realizar negocios; proteger esos recursos es una preocupación principal, ya que la función de los controles y seguridad de la computadora, es proteger los sistemas contra incidentes accidentales, robo intencional, daño de datos y aplicaciones, al igual que ayudar a las organizaciones a asegurar que sus operaciones de tecnología de información, acatan la reglamentación y cumplan con las expectativas de privacidad de los empleados y los clientes, manteniendo la confidencialidad e integridad de la información, adicionando la disponibilidad de los recursos de datos y las operaciones en línea (Derrien,1994)

Dentro los riesgos más frecuentes a los que están expuestos los sistemas de información, están los riesgos para el hardware, y el más importante dentro de este, son los ataques dolorosos de Internet, sumando los daños físicos de la computadora, el equipo periférico y los medios de comunicación; y los causados principalmente por desastres naturales, interrupciones prolongadas del suministro eléctrico, así como el vandalismo. Otro riesgo es para los datos y aplicaciones, los datos recopilados casi nunca se pueden recuperar de la misma manera e incluso cuando esto es posible, el proceso es demasiado costoso y tarda mucho tiempo. La causa más frecuente, es el robo de información y robo de identidad ocasionado por la negligencia de las compañías, por el descuido de la tecnología, sobre todo en las conexiones publicas a internet. La preocupación por las aplicaciones se da casi siempre por personas, y aumenta, cuando estas son personalizadas a los procesos de la organización; otra causa son los virus, gusanos y bombas lógicas, que atacan los datos y las aplicaciones y se extienden de un computador a otro, por medio de archivos compartidos en una red, provocando la restauración total de software y hardware de los computadores, adicionando los percances no

malintencionados que se ocasionan por la falta de capacitación o capacitaciones deficientes que conllevan a ineficiencia en los datos, incumplimiento de procedimientos de respaldo o simples errores humanos(Quijano, R. C. 2006)

Los riesgos también se pueden presentar en las operaciones en línea, por la realización de grandes operaciones a través de internet atrayendo a los intrusos que intentan interrumpir dichas operaciones a diario, pueden darse por accesos no autorizados, el robo de datos y la deformación de las páginas web, han aumentado los ataques de negación del servicio y el secuestro de computadoras (Effy oz, 2006).

Para salvaguardar la información y no poner en riesgo la integridad de los datos y programas instalados por el departamento informático, existen medios de almacenamiento o dispositivos de almacenamiento, cuyo objetivo es permitir la conservación de datos y programas, incluso cuando los equipos no estén conectados a la corriente eléctrica; la diferencia entre estos dos conceptos radica en que el primero es un medio externo y debe considerar el propósito de almacenamiento de los datos, la cantidad de datos que se van a guardar, la velocidad que se requiere para almacenar y la recuperación de los datos, entre ellos están los CD, diskettes, DVD, discos duros y memorias flash; el segundo concepto corresponde al uso de diferentes tecnologías para salvaguardar los datos y la estructura física, entre ellos están las cintas magnéticas y ópticas; otras organizaciones prefieren la utilización de servidores fuera de sus instalaciones, tal es el caso de la empresas multinacionales, que comparten virtualmente una serie de aplicaciones para el uso exclusivo de sus filiales en el mundo, dirigido por un área de tecnología altamente calificada, para ejecutar las políticas y procedimientos de seguridad establecidos por la casa matriz (Montañés y Simon,1999)

Hoy por hoy y con el fin de proporcionar un marco de gestión de la seguridad de la información, utilizable por cualquier compañía independiente de su tamaño o actividad se ha creado un conjunto de estándares, entre ellos está COBIT (objetivos de control para la información y tecnologías relacionadas) desarrollada por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI). Es un modelo internacional que para auditar la gestión y control de los sistemas de información y tecnología generalmente aceptadas, para el uso diario por parte de gestores de negocios y auditores y se considera una de las mejores prácticas, está compuesta por 34 objetivos nivel alto que cubre 215 objetivos de control clasificado en cuatro dominios: el plan y organiza, adquiere y pone en práctica, entrega y apoya, supervisa y evalúa. Entre las organizaciones que lo vienen utilizando estan: La Reserva Federal de los Estados Unidos de América, Daimler en Alemania y en Colombia es un éxito en el Grupo Bancolombia que presta servicios financieros a nivel nacional. (COBIT 4.0)

La norma ISO / IEC 2700 (Information Technology - Security Techniques - Information Security Management Systems - Requirements) Gestión de la seguridad de la información, fue aprobada y publicada como un estándar internacional en el año 2005 por International Organization for Standardization y por la comisión internacional Electrotechnical Commission, es una norma que define los procesos de gestión de la seguridad de la información; para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad informática, con base en el ciclo o modelo Demming PHVA (planear, hacer, verificar, actuar); se compone de 11 dominios, 39 objetivos de seguridad y 133 controles de seguridad, cada dominio se centra en un determinado aspecto de la seguridad de la información. Dentro de esta norma encontramos una serie de estándares que van desde la ISO 2700 hasta ISO 2707. Normas muy

significativas para la implementación de sistemas de gestión de la seguridad de la información. (ISO/IEC 2701: 2009)

Teniendo una conceptualización clara de lo que son los sistemas de información y análisis de riesgos podemos decir que lo difícil no es dimensionar los riesgos a los cuales están sometidos los sistemas de información en las organizaciones y la influencia que tienen dentro de la sociedad que cada vez fluctúan con mayor rapidez, sino la adaptación a los cambios económicos, como los tratados de libre comercio que hacen que las organizaciones, automaticen sus procesos obligándolos a una mejora continua que los lleva a ser competitivos en el mercado. En estas ocasiones, se hace necesario que vayan adoptando aplicaciones que les permitan llegar a una buena toma de decisiones basadas en estadísticas e indicadores y asumir las buenas prácticas de la normatividad existente a nivel internacional y a nivel nacional basados en la norma técnica Colombia 5254 del año 2006. Esta norma nos habla de la gestión de riesgos, conduciendo de esta manera a que las organizaciones sean negocios rentables mejorando la calidad en los servicios y productos; otro cambio importante es la tecnología la cual avanza a pasos agigantados trayendo al mercado herramientas que permiten ser eficaces y eficientes, para las compañías al momento de ser competitivos con sus oponentes; la fidelización de los clientes, mediante el estudio de sus necesidades y el brindar un buen servicio, ser amable , tener un trato cordial, saber escucharlo, prestar atención pos venta, es una condición obligada. Todo esto se traduce a que la información es el eje central de toda compañía y por lo tanto deberá salvaguardarla, como su tesoro más preciado con base en el establecimiento de normas, políticas y procedimientos, que permitan el aseguramiento de información y la exigencia el cumplimiento de las mismas mediante la realización de estudios especializados y la celebración de Jornadas de análisis y debate, tendientes a concientizar a los responsables de procesos de la necesidad de su implicación en las decisiones sobre cómo proteger

adecuadamente la información crítica de su negocio (productos, servicios, clientes, proveedores, empleados y accionistas). Asimismo, estas jornadas tienen como objetivo convertirse en el foro de referencia para el intercambio de experiencia y conocimiento entre los profesionales del sector (Bauza, J1991)

Es evidente que en muchos casos existen ciertas barreras o limitaciones que impiden la implantación de sistemas eficientes de comunicación e información. Por ejemplo, existen instituciones que no disponen de acceso a Internet o este es de baja capacidad. Sin embargo este problema no viene causado por una limitación de la tecnología en sí misma (obviamente, existe tecnología que permite la conexión eficiente a Internet), sino por las dificultades de las instituciones para acceder a ella, por motivos presupuestarios, de recursos humanos, planificación, y otros. Para la implementación de sistemas de información distribuidos, en los que la información circula entre varias instituciones, la fiabilidad de estas conexiones y los servicios implantados en cada institución es una pieza fundamental para la estabilidad del sistema, y por tanto para su aceptación y uso continuado. Sin embargo, muchas entidades tienen dificultades (por limitaciones económicas o de personal) para garantizar la fiabilidad continuada de ciertos sistemas y servicios. Por ello la implantación de cualquier sistema de información, especialmente cuando es distribuido, debe tener en cuenta la necesidad reforzar las capacidades tecnológicas de las instituciones involucradas que garantice en lo posible la fiabilidad de sus servicios. Por otro lado, debe preverse la posibilidad de que se produzcan fallos en el acceso a la información desde su fuente.

Esto significa que para ser exitoso, un sistema de información debe cruzar una multitud de fronteras, no solamente geográficas sino también disciplinares e institucionales. Por esta razón, representantes de los diferentes sectores y niveles deben estar involucrados en todas las fases de desarrollo del sistema, desde el diseño hasta la realización de pruebas y simulacros sobre los riesgos de la

información. Muchos de estos actores se involucrarán también activamente aportando información, implementando servicios y participando en la operación o como destinatarios del sistema de información. Se debe además considerar que el objetivo de la presente discusión no es un sistema de información único sino más bien el refuerzo de una red que agrega multitud de sistemas, unos ya existentes, otros en vías de desarrollo y otros más que se crearían en el futuro. Es esencial por ello el aporte de los representantes técnicos e institucionales de estos sistemas en todas las fases de desarrollo, que aportarían enormemente en la salvaguarda de la información (Scott, 1998).

A menudo solemos oír la frase la seguridad es una cadena que siempre se rompe por el eslabón más débil. La misión de cualquier responsable de Seguridad Informática es la gestión del riesgo sobre los sistemas de información que trata de proteger. Pero, ¿conoce exactamente cuáles son todos los eslabones para poder garantizar la seguridad de la cadena? La fase de análisis y la gestión de riesgos nos ayudan a identificar todos los activos importantes para la seguridad de los sistemas de información, las amenazas que pueden afectarles, identificar la vulnerabilidad de cada uno de ellos frente a estas amenazas y calcular el riesgo existente de un posible impacto sobre el activo. Con toda esta información, el responsable de seguridad puede tomar las decisiones pertinentes para implantar medidas de seguridad en los sistemas optimizando el factor riesgo-inversión.

Es curioso ver como algunos incidentes de seguridad graves se han producido por pequeños fallos en elementos del sistema de información que, respecto a la seguridad, habían sido considerados sin importancia o, no habían sido tenidos en cuenta. Aparece el fenómeno de la bola de nieve, es decir, la acumulación de pequeños errores en sistemas no muy importantes producen al final un incidente de seguridad muy grave, afectando sobre todo los sistemas de información.

¿Por qué se produce este fenómeno? Unas veces, es debido a que en algún momento del diseño de los sistemas de seguridad se descuidaron las medidas de salvaguarda sobre algún elemento de la cadena de fallo, el que al final se convirtió en el eslabón más débil. Otras, ocurre que no se identificaron todas las amenazas que podían afectar al sistema o bien no se estimaron correctamente las vulnerabilidades que el sistema presentaba frente a ciertas amenazas. Y otras veces, no se conocen los niveles de dependencia existentes entre los diferentes elementos del sistema de información, apareciendo efectos colaterales sobre otros elementos no relacionados en primera instancia.

El presente ensayo ha tratado de ilustrar de una forma sencilla en qué consiste el Proceso de Análisis y Gestión de Riesgos descrito por la metodología MAGERIT. Por desgracia, la velocidad a la que se están produciendo los cambios en la gestión de los sistemas de información, nos llevan a tratar de solucionar los problemas de la forma más rápida posible. Estamos contemplando cómo, en materia de Seguridad Informática, este fenómeno está produciendo en algunas organizaciones el descuido en la protección de sus activos. No se llega a entender que actualmente, gran parte del valor de una organización es la información que posee, y que estos activos deben ser protegidos como el preciado valor que tienen, aunque se trate de un elemento difícil de valorar económicamente. Si bien se está realizando un gran esfuerzo, tanto por parte de los profesionales de la informática, como por parte de los directivos de las distintas organizaciones por solucionar esta situación, ello nos lleva sin ninguna duda, a justificar de una forma más contundente la necesaria formalización de las tareas relativas a la Seguridad de la Información (Tomado del articulo análisis y gestión de los riesgos en los sistemas de información publicado en internet en el año 2005 por Javier Cao Avellaneda, Consultor en Seguridad de la Información)

Con lo anterior, se pretende demostrar la importancia de la gestión de riesgos en los sistemas de información, ya que en la actualidad se debe salvaguardar la información con tanto o más celo que en la antigüedad, pues de la información que se tenga de los bienes, productos y servicios, así como de los procesos y procedimientos seguidos para obtenerlos; depende el éxito o fracaso de una organización y por ende de sus competidores.

La pérdida o fuga de información se puede presentar por varios factores entre ellos se encuentra traición de integrantes de la organización quienes venden la información o permiten la fuga de esta, de igual forma no se aplican las medidas de seguridad pertinentes con los sistemas de información; seguido de el continuo ataque de los piratas cibernéticos, y el afán de la competencia por conseguir información de entidades exitosas, sin importar los métodos utilizados para lograr su fin.

Por lo anterior se recomienda realizar estudios especializados y la celebración de Jornadas de análisis y debate, tendientes a concientizar a los responsables de procesos de la necesidad de su implicación en las decisiones sobre cómo proteger adecuadamente la información crítica de su negocio (productos, servicios, clientes, proveedores, empleados y accionistas). Asimismo, estas jornadas tienen como objetivo convertirse en el foro de referencia para el intercambio de experiencia y conocimiento entre los profesionales del sector.

Deben realizarse con un carácter eminentemente práctico, y con la presencia de reconocidos expertos del sector, investigando sobre las experiencias de gestión de riesgos en empresas, y sus estrategias de mitigación, transferencia o aceptación (Bauza, J1991)

REFERENCIAS

Ardebol , Elisenda (2003). *Antropologia de la Religión* . España: Editorial Eureka Media .

Bauza, J. F. (1991). *Administracion de Proyectos* (ciclo de Desarrollo de Sistemas de Informacion). Valencia : Miro C.A.

Cao, Javier (2005). *Análisis y Gestion de los Riesgos en los Sistemas de Información.*

Cocho, J. M. (2003). *Riesgos y seguridad de los sistemas informaticos* . Valencia : Editorial UPV.

Derrien, Y. (1994). *Tecnicas de La Auditoria Informatica* . España : Alfa Omega - Marcambo S.A. .

Effy,Oz. (2006). *Administración de los sistemas de información.* Valencia :Editoria Thomson Learning.

Ponce de León, J. G. (2020). *Introduccion al analisis de Riesgo* . Mexico, D.F.: Editorial Limusa , sa de Cv.

Quijano, R. C. (2006). *Administracion de Riesgos un Enfoque Empresarial*. Medellin-Colombia : Fondo Editorial Universidad EAFIT.

Scott, G. M. (1998). *Principios de Sistemas de informacion* . Mexico : Editorial Mc Graw-Hill .

Simón, R. B. *Auditores de Sistemas de Informacion*. Valencia, camino de la Vera : Servicios de Comunicaciones.

(2005) Wiener, N. (1948). *Cibernetica o El Control y Comunicación en Animales y Maquinas* . Tusquets Editores .

Information Tecnology - Segurity tecniques - *Information security management systems - Requirements*. 2009.(2005). ISO /IEC 2701: