Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento
ISSN: 1690-7515
Depósito legal pp 200402ZU1624
Año 7: No. 2, Mayo-Agosto 2010, pp. 63-81

Cómo citar el artículo (Normas APA):
Bracho, D., Rincón, C. y Acurero, A. (2010). Modelo para la cuantificación del riesgo telemático en una organización. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento*, 7 (2), 63-81

Modelo para la cuantificación del riesgo telemático en una organización

David Bracho[1]
Carlos Rincón[2]
Alfredo Acurero[3]

Resumen

El presente trabajo plantea un modelo que ofrece una aproximación al cálculo de riesgo telemático asumido por las organizaciones públicas y privadas en Venezuela. El desarrollo del modelo integra las variables: a) amenaza conformada por frecuencia e impacto, b) vulnerabilidad compuesta por frecuencia e impacto y c) contramedida constituida por efectividad y cobertura - cumplimiento. La variable activo considera el precio de adquisición del bien y su depreciación. Por último, el modelo propuesto calcula la exposición al riesgo telemático con un margen de error mínimo.

Palabras clave: cuantificación, riesgo telemático, amenaza, vulnerabilidad, contramedida

Recibido: 03-06-10 Aceptado: 22-07-10

[1] Ingeniero en Computación. Profesor del Departamento de Computación. Facultad Experimental de Ciencias (FEC) Universidad del Zulia (LUZ). Maestría en Gerencia de Empresas. Experto en redes en ingeniería telemática.
Correo electrónico: drbracho@luz.edu.ve

[2] Licenciado en Computación. Profesor Asociado de la FEC. Profesor del Departamento de Computación. Magíster en Telemática. Cursante del doctorado en Informática de la Universidad Politécnica de Madrid.
Correo electrónico:crincon@luz.edu.ve

[3] Licenciado en Computación. Profesor Asociado de la FEC. Profesor del Departamento de Computación. Magíster en Gerencia de Empresas. Cursante del doctorado en Informática de la Universidad Politécnica de Madrid.
Correo electrónico: aacurero@luz.edu.ve

Model for Telematics Risk Quantification in an Organization

Abstract

This work introduces a model to offer an approach to risk calculation *telematic* assumed by publics and privates organizations in Venezuela. The development of the model is based on: a) Vulnerability composed by frequency and impact c) Countermeasure conformed by effectiveness and coverage – fulfillment. Asset variable considers the purchase price of the goods and its depreciation. Finally, the proposed model calculates the risk exposure *telematic* a minimal margin of error.

Key words: Quantification, Telematic Risk, Threat, Vulnerability, Countermeasure

Introducción

El incremento en el auge de los suscriptores de Internet para el IV trimestre del año 2009, arrojó la cifra de 2.033.858 usuarios, lo que significó un aumento del 38% con respecto al mismo período durante el año 2008, lo cual refleja la captación de 560.867 de nuevos suscriptores, de acuerdo a la Comisión Nacional de Telecomunicaciones (Conatel, 2010). Por otra parte, según la misma fuente, la estimación de los usuarios de Internet para el IV trimestre del 2009, contabilizó una penetración del 31,20%. Sin embargo, este aumento, que se traduce en mejoras en servicios electrónicos y virtuales para las organizaciones y los usuarios en general, viene acompañado de eventos que atentan contra la seguridad. Estos hechos de inseguridad son cada vez más frecuentes y dañinos, y para finales del año 2008, los incidentes de ataques por exposición a virus informáticos llegaron a representar el 50%, los abusos a los recursos de la red el 44% y el robo de equipos portátiles a un 42%. Eventos como los fraudes telemáticos llegaron a representar el 17%. Los accesos no autorizados, penetración de los sistemas y pérdida de información propietaria representó la cifra de 51%, de acuerdo con Richardson (2009) en el informe correspondiente al CSI *Computer Crime* and *Security Survey*. Sin embargo, cuando las organizaciones implementaron algún tipo de protección en la infraestructura y en las transacciones electrónicas, el retorno en la inversión (ROI) se elevó para el año 2009 a 67.8%, cantidad mayor al 44% mostrado para el año 2008, según Richardson (2009). Es por ello que según Cano (2004) "las inversiones en seguridad informática muestran una constante: fortalecimiento del perímetro de seguridad, actualización de infraestructura de seguridad y administración de la seguridad informática. Mucha de esta inversión se concentra en aspectos de hardware, software y servicios, lo cual sugiere un concepto de seguridad informáti-

ca orientado por el modelo de riesgos y controles, que si bien aporta elementos importantes para el mantenimiento de niveles de seguridad informática adecuados para la realidad de cada organización, limita la comprensión de eventos inesperados que generalmente no encuentran respuesta a los mismos y cuestionan el modelo de seguridad informática de la empresa".

En contraste a lo anterior, cerca del 13% de las organizaciones tanto privadas como públicas no utilizan tecnología alguna de protección ante ataques a la seguridad telemática y dentro de las que usan alguna tecnología cerca del 32% no invierte nada en procesos de entrenamiento para identificar y actuar ante la exposición a algún riesgo telemática, de acuerdo con Richardson (2009). Es por ello que, dependiendo del tipo de exposición al riesgo, las consecuencias varían, incrementando la complejidad y nivel de daño, afectando procesos e incluso la operación del negocio parcial o totalmente Molina (2007).

Como resultado de lo anterior, se hace imprescindible contar con una herramienta que aproxime un valor asociado al cálculo que se genera como producto ante la exposición del riesgo telemático asumido. De acuerdo con Molina (2007), para poder hacer un análisis eficiente del riesgo, se deben considerar las siguientes variables: a) activos; b) amenazas; c) vulnerabilidades y d) contramedidas o mecanismos de seguridad. Variables sustentadas en problemas comunes que afectan la estructuración de la gestión y análisis de riesgos son: a) las amenazas puesto que continúan cambiando en su funcionamiento y consecuencias; b) la inversión en infraestructura no es garantía total de seguridad; c) el verdadero valor al negocio se encuentra en la protección de los datos valiosos corporativos y no los individuales; y d) los generados por sistemas específicos. Es por ello que, de acuerdo con Molina (2007), los criterios básicos convencionales como: a) el perímetro, ya no existe; b) la protección a la infraestructura, no protege al negocio; c) las necesidades del negocio obligan a tomar riesgos, lo cual no ofrece garantía de seguridad mínima y generan dudas sobre si la protección del negocio es importante y si ésta debe estar alineada con las necesidades del mismo. Finalmente, indica Molina (2007) que pareciera que existe un efecto natural en donde, mientras más invierte una organización en seguridad, la sensación de inseguridad no deja de estar presente en los usuarios corporativos.

Finalmente, este trabajo pretende, por una parte, convertirse en una guía de referencia para la cuantificación del riesgo telemático; y por otra, la consolidación en la divulgación y transferencia de conocimientos a través de los aportes hechos en las líneas de investigación de gestión del riesgo telemático y seguridad de aplicaciones bajo ambiente Web.

Evolución del riesgo

La dimensión que ha adquirido el riesgo y su cuantificación en las organizaciones ha hecho que más autores dediquen tiempo a proponer modelos que contribuyan con aproximar la exposición asumida del daño medido en valor monetario. De acuerdo con Cano (2004) la tarea no es fácil dado que generalmente las inversiones en seguridad in-

formática se justifican en función de los riesgos y niveles de riesgos a los que puede o podría estar expuesto una organización, sugiriendo para su estimación una adaptación de la matriz de tipos de inversión en seguridad informática presentada por Remenyi (2000). La matriz sugiere como elementos de análisis dos componentes: riesgo/visibilidad e impacto/ganancia. El primero entendido de la manera tradicional establecida por el modelo de riesgos y controles donde la inversión se concentra en atender las zonas identificadas como de mayor riesgo. El segundo expone la importancia desde el punto de vista del negocio y las ganancias derivadas del mismo. Según Cano (2004) la propuesta de análisis de tipos de inversión no pretende solucionar la problemática de la inversión en seguridad informática, sino que busca sugerir una ruta complementaria entre la función de seguridad y la estrategia del negocio con el fin de aportar más y mayor valor y confianza de parte del usuario sobre la utilización de los productos y/o servicios que provee la organización. Sin embargo, esta matriz no ofrece una fórmula que aproxime numéricamente un cálculo ante la exposición, sino que proporciona una valoración en función de escalas cualitativas, establecidos por los dos parámetros referidos inicialmente.

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión (Proyecto MAGERIT, s/f).

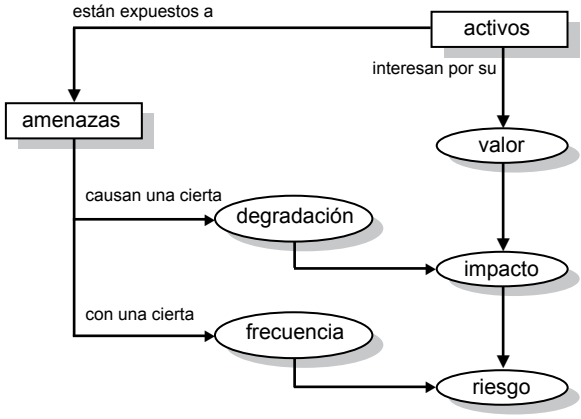
La metodología Magerit acerca del Análisis y Gestión de Riesgos de los Sistemas de Información - versión 2, está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios. Es por ello que, se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. De acuerdo con Magerit, la seguridad se define como "la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles" (Magerit, 2006). Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual es activar medios y esfuerzos para conseguirlas. Las metodologías de análisis y gestión de riesgos exigen precisar algunos términos, tales como: Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Miranda (2009) afirma que riesgo es la probabilidad de que una amenaza llegue a materializarse debido a una vulnerabilidad. Por lo tanto, la amenaza no es más que una persona o cosa vista como posible fuente de peligro. Por otra parte, la Vulnerabilidad es la situación creada, por falta de uno o varios controles, con la que la ame-

naza pudiera materializarse, o como sugiere Magerit, la estimación de la exposición efectiva de un activo a una amenaza.

De acuerdo con Magerit, el análisis de riesgos no es más que el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. El análisis de riesgos permite determinar cómo es, cuánto vale y cuán protegidos se encuentran los activos. Según Miranda (2009), éste indica que facilita la evaluación de los riesgos y recomienda acciones en base al costo-beneficio de las mismas. Asimismo, la Exposición o Impacto, no viene a ser otra cosa que la evaluación del efecto del riesgo. Finalmente, la Gestión de Riesgos se refiere a la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados (Magerit, 2006).

Piattini y García (2007) precisan y establecen los objetivos directos e indirectos de Magerit. Como objetivos directos: a) concienciar a los responsables de los Sistemas de Información (S.I.) de la existencia de riesgos y de la necesidad de atajarlos a tiempo; b) ofrecer un método sistemático para analizar tales riesgos y c) ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Profundizando en el Análisis de Riesgo, dichos autores indican que éste consta de los siguientes procesos: 1) determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación; 2) determinar a qué amenazas están expuestos aquellos activos; 3) determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo; 4) estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza y 5) estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza. La **Figura 1** muestra el diagrama de flujo del proceso de análisis de riesgo.

Figura 1
Análisis de Riesgo



Fuente: Piattini y García (2007)

A pesar de las ventajas de la metodología Magerit existen excepciones interesantes de parte de aquellos profesionales que han decidido elaborar sus "propias" metodologías por considerar que se adaptaban mejor a sus organizaciones que Magerit, en virtud de lo laborioso y costoso que resulta su implementación. Es por ello que la única forma de afrontar la complejidad es centrarse en lo más importante (máximo impacto, máximo

riesgo) y obviar lo que es secundario o incluso despreciable. Adicionalmente, resulta imprescindible contar con una metodología que muestre el tipo de riesgo asumido por cualquier organización privada o pública, personal o jurídica categorizados en: Evitados, Aceptados, Asignados y Atenuados. Según Molina (2007) un tipo de riesgo Evitado es el que evita cualquier contacto con la causa que pueda generar la amenaza. Los Aceptados se dan cuando el costo de la solución es más costoso que el daño y la exposición al riesgo mismo. Los Asignados se generan cuando se cuenta con un tercero que asume las tareas correctivas como consecuencia del daño ocasionado por la amenaza. Por su parte, los Atenuados son aquellos que establecen criterios y medidas de seguridad preventivas y correctivas para reducir el daño causado ante la exposición del riesgo.

Metodología utilizada

La metodología para el análisis de riesgo propuesta por Jarauta, Sierra y Palacios (2006a) establece de forma sencilla procesos y procedimientos a seguir que conllevan a generar un valor cuyo resultado final sea una aproximación ante la exposición al riesgo asumido bien sea por una organización privada o pública, o de índole personal o jurídica, Esta metodología incorpora todos los elementos considerados por la Magerit, pero sin incurrir en detalles complejos en cuanto a minuciosidad. Tampoco hace acepción entre valores acumulados o repercutidos, es decir, para su implementación resulta indiferente el criterio de uso, ventaja que aporta la flexibilidad necesaria para que ésta pueda ser adaptada, sin perder su esencia y naturaleza. Ahora bien, el argumento establecido para modificar dicha metodología radica en la posibilidad de incorporar como mecanismo de cálculo, el corolario de Molina (2007) quien proporciona un modelo matemático sencillo y a su vez no discrimina el procedimiento de cálculo de riesgo de valores, tanto acumulados, como repercutidos. Este modelo puede ser aplicado para ambos casos, dejando a un lado el procedimentalismo y la diferenciación que Magerit exige. Los valores del riesgo acumulado y repercutido, según Piattini y García (2007), se definen como: Riesgo Acumulado: es el calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la frecuencia de la amenaza. Por el contrario, el Riesgo Repercutido: es el calculado sobre un activo teniendo en cuenta el impacto repercutido debido a una amenaza y la frecuencia de la amenaza. Es importante destacar que para los casos de prueba, a pesar de que el corolario no establece consideraciones particulares para cada tipo de riesgo, el criterio establecido para el modelo fue el cálculo de riesgo repercutido por ofrecer condiciones más favorables para su implementación.

En función de lo dicho anteriormente, es importante precisar el nivel de adaptación a la cual fue sometida la metodología de Jarauta, Sierra y Palacios (2006a) y la incorporación del corolario de Molina (2007).

Las etapas de la metodología propuestas por Jarauta, Sierra y Palacios son: 1. Identificación y valoración de activos; 2. Identificación y valoración de las amenazas; 3. Identificación de las medidas de seguridad existentes; 4. Identificación y valoración de vulnerabilidades; 5. Identificación

de restricciones y objetivos de seguridad; 6. Determinar medidas del riesgo; 7. Determinar el impacto; 8. Identificación y seleccionar las medidas de protección.

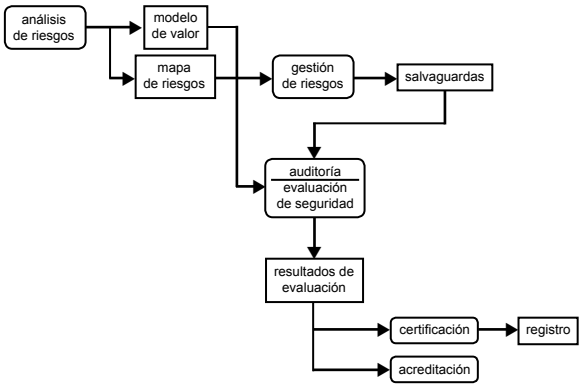
De las siete (7) etapas, la quinta (5) no fue considerada puesto que no aplica para el caso de estudio de riesgo repercutido, ya que se refiere a la identificación de restricciones que persigue: afectan a las medidas de protección a implantar; restricciones de tiempo; financieras; técnicas; sociológicas; ambientales y legales. También se relaciona con los objetivos de seguridad que procura: identificar lo que se espera del plan de seguridad de los sistemas; objetivos estratégicos definidos en la política de seguridad y los objetivos específicos cualitativos y cuantitativos referentes a un activo o grupo de activos.

Al comparar la metodología de Jarauta, Sierra y Palacios (2006a) y la metodología Magerit expuesta por Piattini y García (2007), se aprecia que por ser similares en la estructura, coinciden en cuanto a los criterios de aplicación de las diversas etapas y su propósito. Al respecto, Piattini y García (2007) hacen una acotación importante que determina su aplicación en cualquier caso de uso y es que, estos procesos deben estar definidos previamente a la instalación, configuración y puesta en marcha de algún servicio o producto telemático como parte del trabajo de la alta dirección de cualquier organización, registro que de no contarse ocasiona la pérdida de relevancia y oportunidad del estudio, puesto que, servirá de patrón de referencia o indicador de gestión en procesos de auditoría, certificación y acreditación, tal como lo muestra la **Figura 2**. Por su parte Jarauta, Sierra y Palacios (2006a) sugieren que debe considerarse la omisión y eliminación de las etapas no esenciales para el cálculo de riesgo, puesto que al formar parte de procesos de revisión del negocio éstos no siempre están disponibles, ocasionando distorsión en el valor final obtenido, y generando más trabajo e información inútil que no será usada para el fin requerido.

Debido a lo anteriormente expuesto y a que éste trabajo no aborda los procesos de auditoría, certificación y acreditación, la aplicación de dicha etapa no resulta pertinente considerarla.

Figura 2

Evaluación, Certificación, Auditoría y Acreditación



Fuente: Piattini y García (2007)

Finalmente, Molina (2007) propone un corolario que en principio parece ser más sencillo que la rigurosidad ofrecida por Magerit, pero siempre considerando las mismas variables, tal como, se muestra en la **Fórmula 1**.

Fórmula 1

Corolario

Riesgo **(R)** = Inventario **(I) x** Vulnerabilidad **(V) x** Amenaza **(A) x** Contramedida **(C)**

Fuente: Molina (2007)

Como se aprecia la metodología de Jarauta, Sierra y Palacios (2006a) considera como etapas a desarrollar aquellas que tratan las variables que Molina (2007) refiere en su corolario. La única diferencia radica en la denominación usada por cada autor para referirse al Activo, denominado por Molina (2007) como Inventario y a la Medida de Seguridad, denominada por Molina (2007) como Contramedida.

Desarrollo y aplicación

El modelo de cuantificación de riesgo telemático fue desarrollado mediante el uso de las siguientes herramientas de software: MySQL para realizar el diseño y la creación de la base de datos; Hypertext Preprocessor (PHP) para la programación intermediaria y finalmente WYSISWYG Web Builder 5, para el desarrollo de la interfaz.

Para que el modelo basado en el corolario de Molina (2007) pudiera implementarse fue necesario proponer estructuras de medición de las variables principales que participan en el corolario, las cuales son: Inventario o Activo (I), Amenaza (A), Vulnerabilidad o Debilidad (V) y Mecanismo de Seguridad o Contramedida (C).

Con respecto al inventario, se consideraron de las trece (13) categorías sugeridas por Jarauta, Sierra y Palacios (2006a) sólo aquellas que tuvieran relación directa con elementos computacionales y telemáticos tangibles e intangibles, quedando seleccionadas tres (3) categorías, las cuales fueron: a) Hardware: que considera mainframe, servidores, equipos computacionales, portátiles, entre otros; b) Software que considera sistemas operativos, aplicaciones comerciales y propias, herramientas de desarrollo, base de datos entre otros; y c) Equipos de comunicaciones que considera enrutadores, conmutadores, entre otros. La medición del inventario se hizo en función del precio de compra original y una actualización según el valor del mismo en el mercado, considerando la depreciación del mismo y la revalorización producto del efecto inflacionario.

Para obtener la depreciación del inventario o activo se usó el método de la línea recta. Consiste en dividir el valor del activo entre la vida útil del mismo, esto según Mata (1999), quien también indica que el término vida útil se refiere al período durante el cual se espera que un activo depreciable sea usado por la entidad; o el número de unidades de producción o unidades similares que la entidad espera obtener del activo. Para considerar el efecto inflacionario, hay que entender lo que significa la inflación, la cual, de acuerdo con Sanabria y Ojeda (2002) es el proceso de aumento continuo y generalizado de los precios de los bienes y servicios que se comercializan en la economía. Por lo tanto, lo anteriormente explicado, se muestra en la **Fórmula 2**.

Fórmula 2

Valor del Inventario

$$I_i = \{ I - [(I / V) \times I] \} \times (1 + If_j)$$

Donde I = activo; V = vida útil expresada en unidades de tiempo; i = año;
If= Índice de Precios al Consumidor (IPC) y j= año referido.
Para $0 \leq I$; $0 \leq V$; $0 \leq If \leq 1$.

La unidad que se usó para medir el inventario fue la monetaria, es decir, Bolívares Fuertes (BsF). Es importante resaltar que por considerar unidades monetarias, el modelo puede usarse tanto para casos cuando los activos están expresados en BsF como en cualquier otra unidad monetaria. Lo debe tomarse en cuenta es que deben considerarse para todos los casos las mismas unidades, por lo que fue imprescindible transformar las unidades monetarias usando la referencia o paridad cambiaria BsF/ US$, para aquellos casos cuando los activos fueron adquiridos en el extranjero.

En lo que respecta a la amenaza y considerando la definición aportada anteriormente, se encuentra conformada por dos eventos independientes que son la frecuencia y el impacto, eventos que son referidos y considerados de forma detallada por Magerit (2006). Por frecuencia se entiende la ocurrencia de algún evento, es decir, cada cuánto se materializa una amenaza. Por impacto se entendió como el daño o gravedad del evento, es decir cuan perjudicial pudiera ser la amenaza con respecto al Inventario en cuestión. En virtud que, el Riesgo se expresa como la probabilidad de que una amenaza llegue a ocurrir por una vulnerabilidad, la amenaza también se expresa como la probabilidad en que la frecuencia dañe un activo (Miranda, 2009). Debido a que un activo en particular puede ser objeto de varias amenazas, la fórmula quedó planteada, tal como se aprecia en la **Fórmula 3**: Amenazas.

Fórmula 3

Amenazas

$$A = \sum^{n}_{i=1} (f_i \times i_i) / n$$

Donde A = Amenaza; f = frecuencia; i = impacto y n = nº de amenazas.
Para $0 \leq f \leq 1$ y $0 \leq i \leq 1$.

Para poder considerar el grupo de amenazas totales que pueden afectar a los activos, se usó la tabla de amenazas que registra Richardson (2009), que se muestra en la **Figura 3**.

Es importante indicar que no todas las amenazas afectan a cada activo y, de afectarlo, es necesario particularizar el análisis para aproximar los valores de frecuencia e impacto que se causan. Sin embargo, para esta investigación, se consideró relevante identificar si una amenaza afecta o no a las categorías de activos escogidos, tomando los valores de frecuencia e impacto de la información suministrada por Richardson (2008) y Richardson (2009) puesto que ofrece una muestra representativa y confiable.

En lo que respecta a la vulnerabilidad o debilidad, según su definición se desprende que está conformada por dos eventos independientes que son la frecuencia y el impacto, eventos que

son referidos y considerados de forma detallada por Magerit (2006). Tales eventos son tratados de la misma forma como se trataron cuando de abordó el punto referido a las amenazas. La forma de cuantificar la vulnerabilidad se aprecia en la **Fórmula 4**.

Figura 3
Tipos de ataques

Type of Attack	2005	2006	2007	2008	2009
Malware infection	74%	65%	52%	50%	64%
Bots / zombies within the organization added in 2007			21%	20%	23%
Being fraudulently represented as sender of phishing messages added in 2007			26%	31%	34%
Password sniffing added in 2007			10%	9%	17%
Financial fraud	7%	9%	12%	12%	20%
Denial of service	32%	25%	25%	21%	29%
Extortion or blackmail associated with threat of attack or release of stolen data option added in 2009					3%
Web site defacement	5%	6%	10%	6%	14%
Other exploit of public-facing Web site option altered in 2008					6%
Exploit of wireless network	16%	14%	17%	14%	8%
Exploit of DNS server added in 2007			6%	8%	7%
Exploit of client Web browser option added in 2009					11%
Exploit of user's social network profile option added in 2009					7%
Instant messaging abuse added in 2007			25%	21%	8%
Instant abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Unauthorized access or privilege escalation by insider option altered in 2009					15%
System penetration by outsider option altered in 2009					14%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss option added in 2008				8%	6%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss option added in 2008				4%	6%
Theft of or unauthorized access to PII or PHI due to all other causes option added in 2008				8%	10%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss option added in 2008				5%	8%

Fuente: Richardson (2009)

Fórmula 4

Vulnerabilidad

$$V = \sum_{i=1}^{n} (f_i \times i_i) / n$$

Donde V = Vulnerabilidad; f = frecuencia; i = impacto y n = nº de vulnerabilidad.
Para $0 \leq f \leq 1$ y $0 \leq i \leq 1$.

Para poder considerar el grupo de vulnerabilidades que pueden afectar a los activos, se usó la adaptación de la lista de vulnerabilidades referidas en el estándar ISO 17799 proporcionada por Jarauta, Sierra y Palacios (2006b). Esta adaptación se basó en seleccionar entre las distintas causas que pueden ser consideradas como vulnerabilidades, es decir, aquellas que fueran afines para las tres (3) categorías de activos consideradas para esta investigación. Las vulnerabilidades particulares no fueron consideradas. Las vulnerabilidades escogidas se presentan en la **Figura 4**.

Figura 4

Lista de vulnerabilidades

Mecanismos de Control de Accesos	- Administración de la sesión
	- Validación del ingreso del personal
	- Comprobación inadecuada a los sistemas
	Se bloquean accesos no autorizados a determinados servicios en los servidores de la DMZ.
	- Son realmente seguros los puntos de acceso remoto a la red.
	- Las claves de acceso tienen exceso de privilegios.
	- Se revisan las bitácoras de acceso a la red para vigilar y detectar intentos de acceso no autorizados.
Manejo de data sensible	- Implementación de Algoritmos criptográficos.
Software Antivirus, Sistemas Operativos y Herramientas de Escritorio	- Software antivirus obsoleto.
	- Sistemas configurados incorrectamente.
	- Existen vulnerabilidades de código como desbordamientos de búfer.
	- Los Sistemas no son auditados, supervisados o protegidos.
	- Se aplican los diferentes parches, que los fabricantes de los sistemas operativos publican.
	- Existen aplicaciones que no se han parchado convenientemente, o que no estén actualizadas.
Telecomunicaciones	- Protocolos de red sin cifrar.
	- Existen conexiones a varias redes.
	- Se permiten protocolos obsoletos y fáciles de violar.
	- Sin filtrado entre segmentos de red.

Con respecto a los Mecanismos de Seguridad o Contramedidas, según lo expresado por Molina (2007), éste sugiere que las contramedidas pueden estar conformadas por dos eventos independientes que son la efectividad y la cobertura - cumplimiento. La efectividad queda expresada en términos percentiles, la cual muestra la eficiencia de la herramienta usada como mecanismos de seguridad para proteger a algún activo ante la exposición de amenazas. Por su parte, la cobertura - cumplimiento, también queda expresada en términos percentiles, y se refiere al alcance de la herramienta para garantizar la mayor cantidad de protección ante un número mayor de amenazas. La **Fórmula 5** expresa la forma de cuantificar la contramedida.

Fórmula 5

Contramedidas

$$C = \sum^{n}_{i=1} (Efec_{i} \times CC_{i}) / n$$

Donde C = Contramedida; Efec = efectividad;
CC = cobertura - cumplimiento y
n = nº de contramedidas.
Para $0 \leq f \leq 1$ y $0 \leq i \leq 1$.

Para listar las contramedidas a usar, el criterio utilizado primeramente hizo énfasis en escoger la más comunes e importantes y en segundo lugar, aquellas que estuvieran orientadas a proteger ante la presencia de amenazas generales Molina (2007). Las Herramientas o soluciones particulares no fueron consideradas. A continuación, se muestra la **Figura 5** que recoge las contramedidas consideradas.

Figura 5

Lista de contramedidas

Herramientas de contramedida
Políticas de seguridad
Cortafuegos externos
Cortafuegos internos
IDS
IPS
HIPS
Anti-Virus
Manejo de contenido de URL
Gestión de enrutamiento
Control de acceso de redes
Gestión de SPAM
Anti-Spyware

Fuente: Molina (2007)

Resultados

Con el propósito de mostrar las pruebas obtenidas producto del modelo de cuantificación desarrollado y considerando las excepciones y limitaciones que el corolario de Molina (2007) posee, fue necesario relacionar por cada tipo de activo las amenazas a las cuales éstos son susceptibles, tal como se muestra en la **Figura 6**.

Figura 6

Lista de amenazas por activos

	Activos	Ataques
HARDWARE		- Virus
	- PC	- Acceso no autorizado a la información
	- Laptop	- Robo del cliente / Datos del empleado
	- Servidores	- Fraude financiero
		- Apropiación de contraseña
		- Sabotaje
		- Bots dentro de la organización
SOFTWARE	**Activos**	**Ataques**
	- Sistemas Operativos	- Negación del servicio
	- Aplicaciones propias	- Penetración de sistemas
	- Aplicaciones comerciales	- Fraude financiero
TELECOMUNI-CACIONES	**Activos**	**Ataques**
	- Router	- Fraude de telecomunicaciones
	- Switch	
	- Modem	

Con el fin de determinar el tipo de riesgo asumido fue necesario establecer la procedencia y dependencia de las variables consideradas en el corolario por Molina (2007). La amenaza procede de fuentes externas, es decir, no es controlable por la organización.

En contraparte, las vulnerabilidades y contramedidas tienen una procedencia de origen o fuente interna, puesto que están referidas al hardware y software instalados y en uso que bien pueden ofrecer ventajas o desventajas con respecto a la configuración preestablecida, configuración que pudiera y dependiendo del caso ser una fortaleza o debilidad ante las amenazas que pueden afectar a cada activo en particular.

Considerando esto, Molina (2007) indicó que determinando y valorando las amenazas, las únicas variables que pueden usarse para determinar la exposición al riesgo son las vulnerabilidades y las contramedidas. Es por ello que la exposición al riesgo puede representarse por la relación de contramedidas y vulnerabilidades, relación que es complementaria.

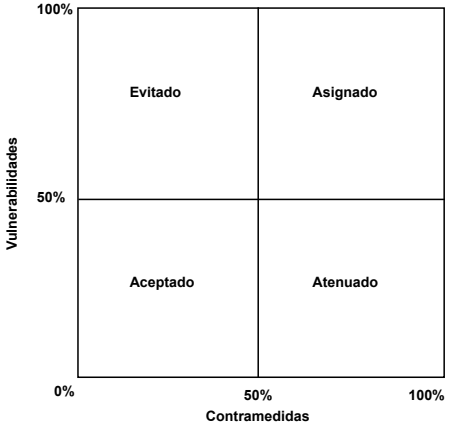
Para nuestro caso de estudio, un valor cercano o igual a 100% para las vulnerabilidades representa una debilidad total, mientras que el valor cercano o igual a 0% representa una ausencia total de debilidad. Para el caso de las contramedidas, un valor cercano o igual al 100% representa una protección total, mientras que un valor cercano o igual al 0% representa una ausencia total de protección. Se estableció como punto medio, es decir el 50% el límite entre los rangos bajos y altos para la clasificación de las vulnerabilidades y contramedidas.

El riesgo Evitado ocurre cuando las debilidades son altas (mayores al 50%) y las contramedidas son bajas (menores al 50%). De ello se desprende que como las herramientas de seguridad no ofrecen las garantías mínimas, la actitud asumida por la organización es evitar la exposición. Por su parte, los riesgos Aceptados ocurren cuando las debilidades son bajas (menores al 50%) y las contramedidas son bajas (menores al 50%) esto se aprecia cuando el daño ocasionado por las amenazas es bajo, ello genera una falsa sensación de seguridad y lleva a las organizaciones a desestimar en invertir en esquemas de seguridad robustos, puesto que, los costos excederían a los daños generados por las Amenazas. Los riesgos Asignados suceden cuando se delega en un tercero las tareas correctivas y/o preventivas, esta tendencia se fortalece cuando las debilidades son altas (mayores al 50%), y pese a que las contramedidas también son altas (mayores al 50%) la propia naturaleza de la organización no contempla disponer de una unidad operativa de seguridad, y en todo caso, de considerarse, éstos serían exageradamente altos, descantando esta alternativa. Por último, los riesgos Atenuados ocurren cuando las contramedidas ofrecen una garantía de seguridad alta (mayores al 50%) y las debilidades en la infraestructura telemática son bajas (menores al 50%), este es el estado ideal donde se invierte en seguridad porque los beneficios de proteger los activos y garantizar su continuidad son mayores que el costo de exponerse a los daños que las Amenazas pudieran ocasionar.

Finalmente, es importante resaltar que las organizaciones con mucha frecuencia afrontan el riesgo no basado en un único enfoque, por el contrario, escogen estrategias que combinan a más de uno de los tipos mencionados, procurando de esta forma obtener la máxima seguridad posible ante las amenazas existentes. La **Figura 7** muestra la relación entre las contramedidas y vulnerabilidades.

Figura 7

Relación de Contramedidas y Vulnerabilidades



Para corroborar la confiabilidad de las pruebas obtenidas por el modelo desarrollado, fueron usados los resultados arrojados por Molina (2007) como parámetros de referencia y de esta forma poder comparar cada uno de los escenarios originales con los que el modelo propuesto arrojó. Es importante resaltar que el caso referido por Molina (2007) no muestra en detalle las cantidades, tipos y valores de los activos trabajados, por el contario, únicamente se centra en indicar los valores consolidados. Al desconocer éstos detalles, fue necesario comparar ambos modelos sobre los valores consolidados y así proceder con la verificación y validación del modelo propuesto en términos de confiabilidad. Esta situación de vació de información fue solventada al escoger una configuración de infraestructura en particular sobre el modelo propuesto la cual debió aproximarse a los valores considerando por Molina (2007). Al encontrar una combinación factible de valores para las amenazas, contramedidas y vulnerabilidades fue posible determinar la exactitud arrojada en el cálculo del riesgo telemático, entendido éste como la diferencias entre ambos modelos, y finalmente determinar si ésta diferencia estaba por debajo del 10%, indicador máximo fijado como parámetro de aceptación final . Las **Figuras 8, 9** y **10** muestran los valores tanto de Molina (2007) como los propios.

Figura 8

Pruebas de cuantificación de riesgo N°1

Cálculo 1	Riesgo	Inventario	Vulnerabilidad	Amenaza	Contramedida
Corolario Molina	$10.357.939,00	$88.842.392,00	25.35%	1	47,88%
Modelo propuesto	$10.661.087,04	$88.842.392,00	25,00%	1	48,00%

Figura 9

Pruebas de cuantificación de riesgo N°2

Cálculo 2	Riesgo	Inventario	Vulnerabilidad	Amenaza	Contramedida
Corolario Molina	$10.124.885,00	$88.842.392,00	20.70%	1	55,06%
Modelo propuesto	$9.866.121,76	$88.842.392,00	20,14%	1	55,14%

Figura 10

Pruebas de cuantificación de riesgo N°3

Cálculo 3	Riesgo	Inventario	Vulnerabilidad	Amenaza	Contramedida
Corolario Molina	$10.124.885,00	$88.842.392,00	20.70%	1	55,06%
Modelo propuesto	$10.261.296,27	$88.842.392,00	21,00%	1	55,00%

Para los tres casos de pruebas realizados, se muestra que el margen de error promedio entre el corolario de Molina y el modelo propuesto fue de 2,28%. La **Figura 11** muestra el error medido como la diferencia entre los valores finales de riesgo dado entre el modelo propuesto y el corolario de Molina (2007).

Figura 11
Margen de error

Margen de error	Corolario Molina	Modelo de propuesto	% de error
Cálculo 1 (Inventario de activos)	$10.357.939,00	$10.661.087,04	2,93%
Cálculo 2 (Análisis de sensibilidad)	$10.124.885,00	$9.866.121,76	2,56%
Cálculo 3 (Inventario de activos)	$10.124.885,00	$10.261.296,27	1,35%

Conclusiones

El conocimiento del riesgo asumido por las organizaciones se ha convertido en un factor crítico de éxito para la competitividad y supervivencia de las mismas. Hoy día, resulta ingenuo desconocer cuál tipo de riesgo se asume y mejor aún cuál debería ser la estrategia a seguir para migrar (si es el caso) de tipo de riesgo o permanecer en una categoría que haga del mismo un elemento manejable y cuantificable. Es obvio que toda organización está sometida a todo tipo de amenazas, las cuales pueden potencialmente afectar el servicio telemático, por ende, el riesgo es una realidad, y así se omita su existencia no se exime de las consecuencias que éstas pueden ocasionar en las organizaciones, es por ello que, las soluciones deben brindar la garantía suficiente que ayude a reducir esa exposición, con el fin de asegurar la continuidad de las operaciones y del servicio telemático. El modelo desarrollado no pretende convertirse en una herramienta única e infalible la cual aplicada correctamente indique detalladamente los pasos a seguir para no ser víctima de alguna amenaza, más bien, contar con ella es una ventaja que bien aplicada es una solución complementaria y robusta que aproxima el cálculo de exposición del riesgo con un margen de error menor al 3%.

Del presente modelo de cuantificación de riesgo y de la relación de las variables que la conforman, se deriva lo siguiente: Con respecto a las amenazas, no se puede tener mayor control por tener su origen externo, pero, sobre las vulnerabilidades y contramedidas sí, por tener éstas su origen interno. Adicionalmente estas dos variables son complementarias. Como consecuencia de lo anterior, las contramedidas y vulnerabilidades son las que determinan el tipo de riesgo asumido,

siendo la relación entre las dos variables inversamente proporcional, es decir, al incrementar las contramedidas se reducen las vulnerabilidades y viceversa.

En virtud de lo anterior los criterios establecidos en función de esta relación fueron: cuando las vulnerabilidades sean menores al 50% y las contramedidas mayores al 50%, las organizaciones están asumiendo un riesgo atenuado. Caso contrario, cuando las vulnerabilidades son mayores al 50% y las contramedidas menores al 50% las organizaciones están asumiendo un riesgo evitado. Cuando las vulnerabilidades y las contramedidas son mayores al 50%, el tipo de riesgo asumido es asignado y cuando las vulnerabilidades y contramedidas son menores al 50% el riesgo asumido es aceptado. Este criterio está seriamente condicionado al costo de la inversión de la solución y su efectividad versus al costo en la pérdida de los activos ocasionada por las amenazas.

Asimismo, dependiendo del tipo de vulnerabilidad y de contramedida puede o no identificarse el tipo de riesgo asumido, pero es más coherente asumir siempre un riesgo con una actitud de atenuación, incluso acompañada con un criterio asignado que haría más robusta la posición de la organización ante la exposición asumida. Sin embargo, cuando no hay posibilidad de hacer frente a alguna amenaza y por ende las soluciones son ineficientes y débiles y el daño puede ser cuantioso, la prudencia prevalece como criterio al evitar el contacto.

Como las vulnerabilidades y las contramedidas son complementarias, cuando se desea disminuir la exposición del riesgo asumido usando el corolario del modelo de cuantificación, la proporción a disminuir debe ser distribuida entre ambas variables, pudiendo una contener un valor mayor que el otro pero nunca asumir a ninguna en la totalidad del valor esperado a disminuir.

Finalmente, y a pesar que cada vez existe mayor dependencia de las organizaciones de los sistemas y servicios telemáticos, no deja de ser un tema recurrente la inquietud por la seguridad. Aquellos usuarios del servicio tienden a cuestionar la confianza de éstos como consecuencia de los problemas y daños ocasionados, incluso a pesar de la cuantiosa inversión hecha en materia de seguridad telemática.

Todo sistema telemático está expuesto al riesgo, por lo tanto, hay que coexistir y tratar con ellos, siendo lo recomendable no sólo poder contar con herramientas y/o soluciones efectivas que con bajo costo contribuyan a reducir el efecto de exposición ante el riesgo, sino que contribuyan con calcular el valor de éste y determinar cuál tipo de riesgo se asume y si ésta posición es la mejor y puede ser mantenida o por el contrario, debe ser corregida a la brevedad posible con el menor efecto en el impacto en los costos o en su defecto con una política escalar pero continua que lleve éste a un valor razonablemente manejable por la organización en cuestión.

Ante esta situación se puede decir que el análisis de riesgos no es una tarea menor que realiza cualquier persona en sus ratos libres. Por el contrario resulta ser una tarea compleja y laboriosa, que exige mucho detalle y esfuerzo.

Bibliografía

Cano, J. (2004). *Apuntes sobre la Inversión y Gestión de la Seguridad Informática*. Recuperado el 12 de julio de 2009 del sitio web Criptored de la Universidad Politécnica de España http://www.criptored.upm.es/paginas/docencia.htm#tematicaGestionDeSeguridad.

Conatel. (2010). *Resultado del Sector Telecomunicaciones IV trimestre 2009*. Recuperado el 22 de abril de 2010 del sitio web de Conatel http://www.conatel.gob.ve/Indicadores/indicadores2009/resultados_al_IV_trimestre_2009.pdf

Jarauta, J. Sierra, J. y Palacios, R. (2006a). *Seguridad Informática: Capítulo 2: Análisis de Riesgos*. Recuperado el 07 de mayo de 2009 del sitio web del Instituto de Investigación Tecnológica de la Escuela Técnica Superior de Ingeniería ICAI de la Universidad Pontificia Comillas http://www.iit.upco.es/palacios/seguridad/cap02.pdf

Jarauta, J. Sierra, J. y Palacios, R. (2006b). *Autodiagnóstico ISO 17799*. Recuperado el 07 de mayo de 2009 del sitio web del Instituto de Investigación Tecnológica de la Escuela Técnica Superior de Ingeniería ICAI de la Universidad Pontificia Comillas http://www.iit.upco.es/palacios/seguridad/p01.zip

Magerit. (2006). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – versión 2*. Recuperado el 15 de septiembre de 2009 del sitio web del Consejo Superior de Administración Electrónica del Ministerio de la Presidencia del Gobierno de España http://www.csi.map.es/csi/pg5m20.htm

Mata, H. (1999). *Cálculo Depreciación con MS Excel*. Recuperado el 14 de junio de 2009 del sitio Web del Profesor de la ULA http://webdelprofesor.ula.ve/economia/hmata/Notas/C%E1lculo%20Depreciaci%F3n%20con%20MS%20Excel.pdf

Molina, D. (2007). *Modelo Económico para la Administración de Riesgos – Madurando a "Security 2.0"*. Recuperado el 13 de junio de 2009 del sitio web Business Innovation Forum http://www.innovationforum.com.mx/e2007/presentaciones/bif07_keynoteMcAfee.pdf

Miranda, E. (2009) *Tema 4: Metodologías de control interno, seguridad y auditoría informática*. Recuperado el 25 de Junio de 2009 del sitio web de Facultad de Ciencias Contalbes y Financieras de la Universidad Nacional Jorge Basadre Grohomann http://facf.unjbg.edu.pe/docentes/e_miranda.html

Piattini, M. y García, I. (2007). *Análisis y Gestión de Riesgos*. Recuperado el 06 de Junio de 2009 del sitio web Auditoría y Seguridad de Sistemas de Información del grupo Alarcos de la Universidad Castilla – La Mancha http://alarcos.esi.uclm.es/doc/Auditoria/ASI22.ppt

Proyecto MAGERIT (s/f). *Methodology for Information Systems Risk Analysis and Management*. En Ministerio de Administraciones Públicas, (2006). Recuperado el 15 de julio de 2010 del sitio web del Consejo Superior de Administración Electrónica del Ministerio de la Presidencia del Gobierno de España http://www.csi.map.es/csi/pg5m20.htm

Remenyi, D.; Money, A.; Sherwood-Smith, M; y Irani, Z. (2000). *The effective measurement and management of IT Cost and benefits*. Recuperado el 22 de Julio de 2009 del sitio web Google académico http://books.google.co.ve/books?hl=es&lr=&id=vEIic3AAPTwC&oi=fnd&pg=PR11&dq=The+effective+measurement+and+management+of+IT+Cost+and+benefits&ots=Nw7CL22wkp&sig=prtOCYZc42Ts1P8MPi7CtqD07VQ#v=onepage&q=The%20effective%20measurement%20and%20management%20of%20IT%20Cost%20and%20benefits&f=false

Richardson, R. (2008). *2008 CSI Computer Crime and Security Survey*. Recuperado el 8 de febrero de 2010 del sitio web CSI http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf

Richardson, R. (2009). *14th Annual CSI Computer Crime and Security Survey. Executive Summary*. Recuperado el 12 de marzo de 2010 del sitio web CSI http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey09_Executive-Summary.pdf

Sanabria, B. y Ojeda, Y. (2002). *La Inflación y el Índice de Precios al Consumidor, base 1997***.** Recuperado el 17 de mayo de 2009 del sitio web de Banco Central de Venezuela http://www.bcv.org.ve/Upload/Publicaciones/cuaderno3.pdf