Validación de un método ágil para el análisis de riesgos de la información digital*

Validation of an Agile Method for Risk Analysis of Digital Information

Luis Merchán Paredes
Diego Gómez Mosquera

Resumen

Frecuentemente se observa en las pequeñas empresas de tecnología la carencia de una cultura de análisis de riesgo para los activos digitales; en gran medida, debido al alto costo de la implementación de métodos conocidos que requieren compromisos en tiempo y esfuerzo que muchas veces superan la capacidad empresarial. Por ello se diseñó y validó un método que de manera ágil permite a las pequeñas empresas implantar el análisis de riesgo de la información digital en sus procesos. El método evita la destinación excesiva de recursos que es característica de los métodos y metodologías tradicionales.

El método y su herramienta informática se aplicaron y validaron en cinco empresas con características diferentes. Los resultados fueron satisfactorios, como lo reflejan los indicadores de productividad, eficiencia y efectividad desarrollados para evaluar el diseño experimental aplicado.

Palabras clave: activos digitales, análisis de riesgo, empresas de base tecnológica.

Abstract

The lack of a culture of risk analysis for digital assets can be frequently observed in small technology businesses. In large part, this is due to the high cost of implementation using known methods that require sacrifices in time and effort and that, in many cases, are greater than a business's capacities.

This is why a method was designed and validated that allows small businesses to include risk analysis of digital information in their processes. The method avoids excessive consumption of resources, a characteristic of traditional methods and methodologies.

The implementation and validation of the method and its information technology tools were applied

• Fecha de recepción del artículo: 03-08-2011 • Fecha de aceptación: 10-09-2011.

LUIS MERCHÁN PAREDES. Ingeniero de Sistemas de la Universidad Industrial de Santander, Bucaramanga, Colombia, Especialista en Finanzas de la Universidad EAFIT, Medellín, Colombia; Magíster en Administración de Empresas de la Universidad Icesi, Cali, Colombia y Ph.D en Dirección de Proyectos de la Universidad de Zaragoza, España. Profesor de la Facultad de Ingeniería de la Universidad de San Buenaventura, sede Cali. Investigador del Laboratorio de Investigación para el Desarrollo de Ingeniería de Software – LIDIS. Correo electrónico: lmerchan@usbcali.edu.co. **DIEGO GÓMEZ MOSQUERA.** Ingeniero de Sistemas con énfasis en Ingeniería de Software de la Universidad de San Buenaventura Cali. Magíster en Ingeniería de Software de la Universidad Politécnica de Madrid España. Sun Certified Java Programmer. Sun Certified Web Component Developer. Sun Certified Business Component Developer Enterprise Edition 5. Investigador del Laboratorio de Investigación para el Desarrollo de Ingeniería de Software – LIDIS. Profesor del Programa de Ingeniería de Sistemas Universidad de San Buenaventura Cali. Correo electrónico: dagmosq@usbcali.edu.co.

* Se agradece a la Universidad de San Buenaventura por el apoyo recibido para adelantar la presente investigación, así como a las empresas de base tecnológica por su participación y compromiso en el desarrollo y validación del método durante el año 2010. Se reconoce igualmente a los estudiantes Andrés Romero, Mario Acosta, Jefferson Escobar y Noé Laguna el trabajo de desarrollo del *software* que soporta el método.

in five businesses with different characteristics. The satisfactory results were reflected in the indicators for productivity, efficiency and effectiveness that were designed in the context of applied experimental design.

Keywords: *digital assets, risk analysis, grass roots technology businesses.*

Introducción

La mayoría de las pequeñas empresas de tecnología enfrentan riesgos por falta de control de la seguridad de la información, pues suponen que con la aplicación de ciertas medidas (procesos de respaldo) es más que suficiente. Incluso, consideran erróneamente que todos los riesgos posibles están previstos en el plan de riesgos del proyecto (Merchán, 2010:27).

Las empresas deben entender que una buena política con respecto al riesgo en activos digitales debe considerar: 1) la clara identificación de los activos; 2) la valoración de sus impactos en la organización; 3) la identificación de riesgos y el análisis de cómo dichas amenazas afectan los activos; y 4) la correcta elaboración, seguimiento y control sobre las acciones tomadas (ISO/IEC 27001:22). Lo anterior se puede lograr a través de un adecuado diseño de instrumentos que permita responder a interrogantes como: ¿Cuáles son los activos de información más valiosos? ¿Cuál es el nivel de exposición de los activos? ¿Cómo actuar preventivamente? ¿Cómo reaccionar ante eventos que afecten la integridad de los activos digitales?

El objetivo central del proyecto fue diseñar y desarrollar, sobre una base aplicativa de conocimiento, un conjunto de métodos y prácticas que permitiera a las pequeñas empresas administrar de manera ágil los recursos y procesos vinculados a un Sistema de Gestión de Seguridad de la Información (SGSI).

El producto final del proyecto permite la generación de información comparable con otros procesos de análisis de riesgos de activos digitales o con evoluciones cíclicas del riesgo. Los indicadores propuestos son una herramienta de apoyo a la gestión y a la generación de conocimiento en el proceso de administración de la información digital.

Planteamiento del problema

Muchas de las empresas pequeñas de tecnología no realizan pruebas de seguridad que garanticen la confiabilidad de sus procesos o de su información. Esto se debe a diversos motivos, entre los cuales podemos enumerar los siguientes:

- Desconocimiento parcial o total de los métodos y la documentación que el aseguramiento de la información digital implica.
- Entender equivocadamente que la gestión de la seguridad de la información es un problema de gestión de copias de seguridad.
- Imaginarios en los cuales se consideran exentos de eventualidades con la información digital.
- Certeza de que como no les ha pasado nada, nada les puede ocurrir y que, de todas formas, más adelante la empresa entrará a considerar estos aspectos.

La no aplicación de buenas prácticas de aseguramiento de la información digital compromete la confiabilidad de los productos desarrollados y, eventualmente, deteriora la confianza de los clientes en el desarrollo de productos y servicios. Por el contrario, la aplicación de metodologías de gestión de riesgos genera beneficios que impactan el éxito de los proyectos (Hillson, 2007: 7).

La garantía de seguridad y confiabilidad en los procesos de la empresa es un activo intangible de ella. Este valor agregado no suele ser considerado con la seriedad que amerita debido a los costos que dicho proceso de aseguramiento demanda.

Así mismo, a pesar de los innumerables casos ocurridos de infiltración de la información en las empresas, muchas no adoptan políticas, procedimientos ni métodos para mitigar los riesgos inherentes al manejo de la información digital, y en otros casos dichas políticas y procedimientos se enfocan en actividades que no requieran consumo de recursos en esta dirección.

De otra parte, para muchas empresas el problema no es la falta de conocimiento o la incorrecta

aplicación del control sobre la seguridad de la información digital, sino la ausencia de un seguimiento adecuado a los resultados de estos procesos.

El método desarrollado busca que se adopten buenas prácticas de análisis de riesgo de la información digital, acordes con estándares internacionales, que les permitan a las empresas garantizar la calidad de sus productos y servicios y, por tanto, que sean consideradas por ellas como un activo importante.

Referente teórico

En el 2005, la Organización Internacional para la Normalización (ISO) oficializó la norma ISO 27001:2005, conocida como "Sistema de Gestión de Seguridad de la Información", SGSI, y la definió como "[…] la parte del sistema de gestión global basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información" (Alexánder, 2007: 19).

La colección de estándares establecidos y publicados por ISO en octubre de 2005 normaliza y certifica los procesos de los SGSI, promulgados anteriormente por los estándares BS 7799 (1979) e ISO/IEC 1799 (2005). Como complemento a los estándares anteriores, esta colección define parámetros de medición, criterios de evaluación y mecanismos de seguridad.

La colección de los componentes de la familia ISO 27000 se detalla en la Tabla 1 (Alexánder, 2007: 19 y 20):

Tabla 1
Normas de la serie ISO 27000

IDENTIFICACIÓN	TÍTULO
ISO 27000	Vocabulario y definiciones.
ISO 27001	Estándar certificable ya oficializado
ISO 27002	Código de buenas prácticas para la gestión de la seguridad de la información
ISO 27003	Guía para la implementación
ISO 27004	Métricas e indicadores
ISO 27005	Gestión de riesgos de la seguridad de la información
ISO 27006	Requerimientos para entidades que proveen servicios de auditoria

El modelo utilizado por este estándar para la realización de los procesos SGSI se basa en el ciclo *Deming PDCA* (*Plan-Do-Check-Act*), que es el mismo utilizado por las normas ISO9000 e ISO140001.

Para la investigación se asumió como fuente el estándar ISO 27001:2005 y documentos sobre métodos y metodologías propuestos (Alexánder, 2007: 19 y 20), a partir de los cuales se construyó un método ágil que lo soportara para el caso de pequeñas empresas.

Entre los métodos de análisis de riesgo existentes en la actualidad, los siguientes son algunos de los utilizados para el análisis de riesgos sobre activos de información: el método Margerit (Margerit, 1999: 16-31) y los métodos de análisis de riesgos cuantitativos dados por el *National Institute of Standards and Technology* –NIST SP 800-30, NIST SP 800-39 y NIST SP 800-60–, que apoyan el proceso de gestión de riesgos de activos informáticos; pero su robustez, una propiedad interesante, es a su vez una limitante para su aplicación en pequeñas empresas con altas limitaciones de recursos humanos.

Método propuesto

La Figura 1 presenta el método propuesto con una definida orientación en la iteración en la gestión de riesgos y no en el análisis secuencial y metódico de riesgos como lo abordan muchos de los métodos reconocidos.

A continuación se detallan los componentes del método:

Etapa de planeación del SGSI

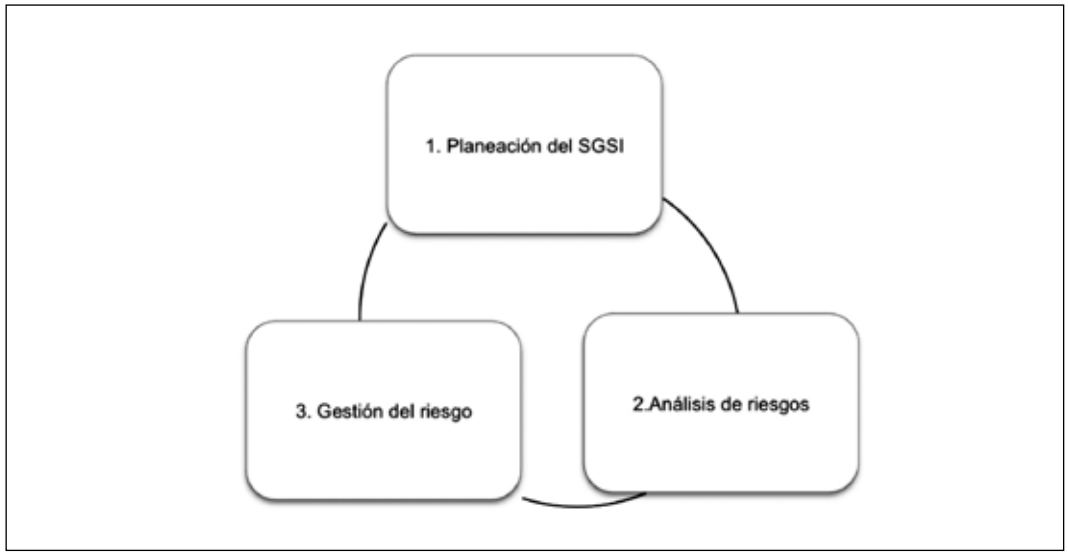
Definir y tipificar procesos

Tiene por objetivo realizar el mapeo de procesos de la cadena de valor de la empresa, que permitirá definir las actividades que le generan ventaja competitiva (crean valor en la cadena), lo que redunda en maximización del valor y minimización de costos. Es el punto de partida del análisis de riesgos.

Definir y tipificar activos

A partir de los procesos/procedimientos de la cadena de valor se deberá realizar un inventario

Figura 1
Método propuesto



completo de los activos que manipulan información y establecer una tipificación de activos que responda a la cadena de valor definida anteriormente. A esta tipificación de activos se deberá asignar, para cada tipo particular de activo, un conjunto de amenazas comunes a todos los activos relacionados en la tipificación. Para efectos de este método, la tipificación de activos utilizada fue la propuesta por el método *Margerit* (Margerit, 1999: 17-22).

Definir amenazas vinculadas

Una vez tipificados los activos se procede a determinar qué amenazas van a ser consideradas en el análisis; dicho listado de amenazas puede ser recolectado por diferentes medios como lluvia de ideas, análisis de experiencias, mecanismos *whatif*, encuestas, entre otros. Para efectos de agilizar el proceso de análisis de riesgos el método sugiere un mapa de amenazas particular para los activos de información digital que responde de manera satisfactoria a las demandas de información solicitadas por los estándares de aseguramiento de información ISO 27001 y BS1229.

Etapa de análisis de riesgos

Determinación del valor de los activos asociados

El valor real de un activo se determina a partir de los costos generados por su falla, teniendo presente que para esto se acumulan los costos de activos precedentes en la respectiva cadena de valor (dependencia directa, indirecta o colateral). A continuación se presenta la fórmula para el respectivo cálculo:

$$VRA = \sum VPR * FR$$

VRA = Valor real del activo

VRP = Valor real de procesos asociados

FR = Frecuencia de relación de asociación

Determinación del valor de impacto real de las amenazas

El siguiente paso es determinar en qué medida estas amenazas afectan los activos y cómo ellas pueden aparecer durante el proceso. El método utiliza para esta determinación el valor probable de daño generable por una amenaza y la posibilidad de que la amenaza se materialice.

Determinación de la severidad de las amenazas sobre activos

Es el cálculo del valor del daño sobre el activo en el caso de que se produzca. En muchas ocasiones el daño es cuantificado por el costo de los procesos de la cadena de valor que se ven afectados por la materialización de la amenaza. Primero se deter-

mina el impacto de la amenaza sobre el activo y luego la severidad de la amenaza, como se describe en las siguientes fórmulas:

$$IPA = \frac{(\Sigma\ DAD * VAD)}{VADmax} / \ ND$$

IPA = Impacto ponderado sobre el activo

DAD = Disponibilidad de amenaza sobre la dimensión de riesgo

VAD = Valoración del activo en la dimensión de riesgo

VADmáx = Máxima valoración del activo en la dimensión posible

ND = Número de dimensiones del riesgo

$$SA = IPA * VRA$$

SA = Severidad de la amenaza sobre el activo

IPA = Impacto ponderado sobre el activo

VRA = Valor real del activo

Determinación de la propensión de las amenazas

Para no entrar en estudios de comportamientos pasados o simulados en circunstancias controladas, el método propone orientar la definición global de la propensión de la amenaza y a partir de ahí calcular el valor como el producto de cuántos puntos dentro del conjunto total de activos podrían en cierto momento materializar una amenaza.

$$P\,(An) = \frac{\Sigma\ An}{TPA}$$

P(An) = Probabilidad de ocurrencia

An = Puntos de amenaza particular "N" por activo

TPA = Total de puntos de amenaza

Determinación del valor del riesgo

El valor del riesgo está determinado por la probabilidad de que una amenaza se materialice y cause daños a los activos de la cadena de valor de la empresa.

$$R_{activo} = \sum SAn * P\,(An)$$

R_{activo} = Riesgo de un activo

SAn = Severidad de la amenaza N sobre el activo

P(An) = Probabilidad de ocurrencia

Determinación del valor de mitigación de las protecciones

Parte de la determinación del impacto de mitigación sobre el activo, para proceder luego a establecer su valor real.

$$MPA = \frac{\Sigma \frac{DMD * VAD}{DMDmax * VADmax}}{ND}$$

MPA = Mitigación ponderada sobre el activo

DMD = Disponibilidad de mitigación sobre la dimensión del riesgo

VAD = Valoración del activo en la dimensión del riesgo

VADmáx = Máxima valoración del activo en la dimensión posible

DMDmáx = Máxima disponibilidad de mitigación sobre la dimensión del riesgo

ND = Número de dimensiones del riesgo

$$SM = MPA * VRA$$

SM = Severidad de la mitigación sobre el activo

MPA = Mitigación ponderada sobre el activo

VRA = Valor real del activo

Determinación de la sensibilización del riesgo

Es el mecanismo que el método brinda como instrumento para permitir analizar diferentes perspectivas y escenarios. Para ello, el método presenta una matriz de sensibilidad de riesgo estandarizada

(ver Tabla 2) que anula aquellos riesgos que no sean de severidad baja (poco impacto en la organización) y de frecuencia baja (poco propensos a ocurrir), y que incrementa considerablemente el valor de los riesgos con severidades y frecuencias medias y altas.

– Baja (entre 0% y 25%)

– Media (mayor a 25% y menor a 75%)

– Alta (mayor a 75%)

Tabla 2
Matriz de sensibilización del riesgo

SEVERIDAD (IMPACTO A LA ORGANIZACIÓN)	FRECUENCIA (PROPENSIÓN A OCURRIR)		
	BAJA	MEDIA	ALTA
Baja	0	3	5
Media	3	5	7
Alta	5	7	10

Gestión de riesgos

La gestión de riesgos se basa en la agrupación de la información recolectada en la etapa anterior y en el respectivo agrupamiento (mapas de riesgos) que se relaciona a continuación:

Mapa de riesgos por proceso

$$RTP = \frac{(\Sigma\ R_{activo}) * VRP}{\Sigma\ VRP}$$

RTP = Riesgo total por proceso

R_{activo} = Riesgo por activo vinculado al proceso

VRP = Valor real del proceso

∑VRP = Sumatoria del valor real de los procesos

Los valores resultado del riesgo por proceso permiten analizar la generación de riesgos por cada proceso del sistema y, por tanto, considerar en cuáles procesos se deben concentrar los esfuerzos de mitigación de acuerdo con el nivel de riesgo que ellos representen para la organización.

Mapa de riesgos por tipo de activo

$$RTTA = (\sum R_{activo}$$

RTTA = Riesgo total por tipo de activo

R_{activo} = Riesgo por activo

Permite al usuario valorar qué tipo de protecciones deben ser instauradas de manera inmediata y filtrar los riesgos generados por los activos de una tipología que permita aplicar una misma medida de protección a varios activos del mismo tipo, economizando con ello labor en la gestión del riesgo.

Mapa de riesgos por activo

$$R_{activo} = \sum SAn * P\,(An)$$

R_{activo} = Riesgo de un activo

SAn = Severidad de la amenaza N sobre el activo

P(An) = Probabilidad de ocurrencia

Permite conocer la situación particular de cada uno de los activos involucrados en el análisis. Este mapa es más una especificación de los mapas anteriores y su utilidad radica principalmente en la determinación del resultado (en el caso de que sea mitigado) de la aplicación de las protecciones involucradas en el análisis. Otro elemento de valor que se puede caracterizar de este mapa es que permite, a su vez, detectar de manera particular cuáles activos representan mayor riesgo para la organización.

Mapa de riesgos por tipo de amenaza

$$RTCA = (\sum R_{amenaza})$$

RTCA = Riesgo total por clase de amenaza

$R_{amenaza}$ = Riesgo por amenaza de la clase

Los valores resultado del riesgo por tipo de amenaza permiten verificar qué comportamientos de amenazas son más dañinos para el proceso organizacional. Al reconocer qué conjuntos de

amenazas significan mayor vulnerabilidad, se puede así mismo identificar con mayor precisión qué tipo de protecciones generarán mayores efectos positivos en el proceso organizacional.

Mapa de riesgos por amenaza

$$R_{amenaza} = \sum SAi * P(An)$$

$R_{amenaza}$ = Riesgo generado por una amenaza

SAi = Severidad de la amenaza por activo

P(An) = Probabilidad de ocurrencia

Los valores resultado del riesgo por amenaza permiten conocer el comportamiento particular de cada amenaza catalogada en el análisis. Este mapa se realiza principalmente como una especificación de los mapas anteriores y su utilidad radica básicamente en la determinación del resultado (en el caso de que sea mitigado) de la aplicación de las protecciones involucradas en el análisis, además de que permite la detección específica de las amenazas más peligrosas para el ámbito organizacional analizado.

Mapas de riesgos dimensionales

$$RPDn = \frac{\Sigma\ RDN_{activo} * VRP}{\Sigma\ VRP}$$

RPDn = Riesgo del proceso por dimensión

RDn_{activo} = Riesgo en la dimensión por activo vinculado al proceso

VRP = Valor real de proceso

VRP = Sumatoria del valor real de los procesos

$$RDnTA = (\sum RDn_{activo})$$

RTTA = Riesgo del tipo de activo por dimensión

RDn_{activo} = Riesgo en la dimensión por activo

$$RDn_{activo} = \sum SAn * P(An)$$

RDn_{activo} = Riesgo en la dimensión por activo

SDAn = Severidad en la dimensión de la amenaza n sobre el activo

P(An) = Probabilidad de ocurrencia

$$RDCA = (\sum RDn_{amenaza})$$

RDCA = Riesgo dimensional por clase de amenaza

$RDn_{amenaza}$ = Riesgo dimensional por amenaza de la clase

$$RDn_{amenaza} = \sum SAi * P(An)$$

$RDn_{amenaza}$ = Riesgo dimensional generado por una amenaza

SDAi = Severidad de la amenaza en la dimensión por activo

P(An) = Probabilidad de ocurrencia

Los valores resultado del riesgo por dimensión permiten especificar la naturaleza del comportamiento del riesgo en cada uno de los escenarios en los que se aplique; de esta manera, se puede determinar, de acuerdo con la necesidad, si el riesgo puede ser considerado en el valor que arroja el análisis totalizado o si debe ser visto en su comportamiento dimensional, según los objetivos que se busquen en el análisis.

Resultados y análisis

A partir del anterior método se procedió a desarrollar una herramienta de programa que soportara el proceso de aplicación en las empresas seleccionadas.

Para la validación del método se diseñó un experimento con los siguientes indicadores:

Indicador de productividad

Tabla3
Porcentaje de riesgos primarios

PORCENTAJE DE RIESGOS PRIMARIOS DETECTADOS	
DESCRIPCIÓN	Indicador que muestra qué tantos de los riesgos detectados son de orden primario o de atención inmediata.
OBJETIVO	Ponderar qué porcentaje del riesgo requiere atención inmediata.
UNIDAD	Porcentual.
FÓRMULA	$\frac{\#\ Riesgos\ con\ valor\ superior\ al\ 50\%\ del\ máximo\ valor\ de\ riesgo}{\#\ Total\ de\ riesgos\ detectados} \times 100\%$
PUNTOS DE MEDICIÓN	Al final de cada ciclo de análisis de riesgos realizado.

Tabla 4
Porcentaje de riesgos secundarios

PORCENTAJE DE RIESGOS SECUNDARIOS DETECTADOS	
DESCRIPCIÓN	Indicador que muestra qué tantos de los riesgos detectados son de orden secundario o qué no requieren de atención inmediata.
OBJETIVO	Ponderar qué porcentaje del riesgo no requiere atención inmediata.
UNIDAD	Porcentual.
FÓRMULA	$\frac{\#\ Riesgos\ con\ valor\ inferior\ al\ 50\%\ del\ máximo\ valor\ de\ riesgo}{\#\ Total\ de\ riesgos\ detectados} \times 100\%$
PUNTOS DE MEDICIÓN	Al final de cada análisis de riesgos.

Indicador de efectividad

Tabla 5
Porcentaje de conocimiento agregado sobre amenazas

PORCENTAJE DE CONOCIMIENTO AGREGADO SOBRE AMENAZAS DESCUBIERTAS	
DESCRIPCIÓN	Indicador que muestra el valor agregado de conocimiento que se genera con la aplicación del método en la empresa.
OBJETIVO	Medir el valor agregado de conocimiento que se genera con la aplicación del método.
UNIDAD	Porcentual.
FÓRMULA	$\frac{\#\ Riesgos\ detectados\ desconocidos\ por\ el\ usuario}{\#\ Total\ de\ riesgos\ detectados} \times 100\%$
PUNTOS DE MEDICIÓN	Al final del análisis de riesgos.

Indicadores de eficiencia

Tabla 6
Tiempo de análisis promedio por proceso

TIEMPO DE ANÁLISIS PROMEDIO POR PROCESO	
DESCRIPCIÓN	Indicador que mide el tiempo que toma realizar un análisis por empresa.
OBJETIVO	Generar métricas de comportamiento para estimar esfuerzos de equipo en futuros análisis.
UNIDAD	Horas / Proceso
FÓRMULA	$\frac{\#\ Horas\ utilizadas\ en\ el\ análisis}{\#\ Total\ de\ procesos\ analizados}$
PUNTOS DE MEDICIÓN	Al final del análisis de riesgos.

Tabla 7
Tiempo de análisis, promedio por activo

TIEMPO DE ANÁLISIS PROMEDIO POR ACTIVO	
DESCRIPCIÓN	Indicador que mide el tiempo que toma realizar un análisis por activo asociado a la empresa.
OBJETIVO	Generar métricas de comportamiento para estimar esfuerzos de equipo en futuros análisis.
UNIDAD	Horas / Activo
FÓRMULA	$\frac{\#\ Horas\ utilizadas\ en\ el\ análisis}{\#\ Total\ de\ activos\ analizados}$
PUNTOS DE MEDICIÓN	Al final del análisis de riesgos.

Dimensión del sistema organizacional de la empresa

Se relaciona a continuación un esquema de valoración de dimensión organizacional para determinar su influencia en el método de acuerdo con su robustez y complejidad. Esta clasificación define el número de procesos y el número de activos que se indexaron en el análisis, y se clasificó de la siguiente manera:

- Empresa pequeña(EP)
- Empresa mediana (EM)
- Empresa grande(EG)

Tabla 8
Esquema de dimensión organizacional

NÚMERO DE ACTIVOS	NÚMERO DE PROCESOS			
		1 a 5	6 a 10	11 ó más
	1 a 20	EP	EP	EM
	21 a 60	EM	EM	EG
	61 ó más	EM	EG	EG

Madurez del sistema organizacional de la empresa

Esta clasificación define el nivel de conocimiento que tiene la empresa sobre su sistema organizacional, y la clasificación depende de cuántos puntos de revisión tenga cumplidos:

- Que tenga establecido el mapa de procesos.
- Que tenga realizado el inventario de activos.
- Que tenga inventariada la actividad de los activos en los procesos.
- Que tenga valorada la importancia de los activos en las diferentes dimensiones de riesgo establecidas.
- Que tenga procesos de análisis de riesgos.

De acuerdo con los anteriores criterios se estableció la siguiente ponderación:

- Empresa de poca madurez (EPM): 0 a 1 puntos de revisión.
- Empresa de mediana madurez (EMM): de 2 a 3 puntos de revisión.
- Empresa de gran madurez (EGM): 4 puntos de revisión o más.

Resultados

Para la validación práctica del método se seleccionaron cinco empresas (dos por tipo de dimensión organizacional), y se obtuvieron los siguientes resultados:

Productividad

Se puede observar que el impacto mayor en productividad se logra en las empresas pequeñas, porque el método aplicado les ayuda, en primera instancia, a organizar sus procesos (mapa de procesos), lo que conduce a poder identificar proactivamente sus riesgos potenciales y, de esta forma, establecer sus acciones de prevención y mitigación. Igualmente, como no aplican buenas prácticas, existen riesgos primarios en mayor proporción que van desapareciendo en la medida que avanzan en madurez.

Efectividad

El método reportó su mayor efectividad en la medida en que el grado de madurez organizacional era inferior.

Eficiencia

La eficiente aplicación del método depende en gran parte del grado de madurez. Es decir, la empresa pequeña por su inmadurez requiere más tiempo para la implementación y, como es lógico, las más maduras pueden realizar el proceso en tiempos mucho más cortos en comparación con tiempos referenciados. Ahora bien, los tiempos reportados en la implementación son mínimos en comparación con los efectos que puede tener el que las empresas tecnológicas no cuenten con este método.

Los resultados de las seis implementaciones muestran claramente que el método generado a partir de la investigación y soportado por el programa desarrollado contribuye a implantar procesos de mejoramiento y a adoptar mejores prácticas que deben conducir al objetivo de crear una industria tecnológica más desarrollada.

Conclusiones y trabajos futuros

La implementación de una buena política de análisis de riesgos de información digital preventiva es no sólo un gran valor agregado para las empresas, sino un conocimiento que aporta a la madurez del proceso organizacional.

Las pequeñas empresas requieren métodos que consulten la realidad sin invertir gran cantidad de recursos o esfuerzos. Todo método orientado a las pequeñas empresas debe tratar de mostrar de manera estandarizada una versión aproximada de la realidad parametrizada por los aspectos particulares de la pequeña empresa.

Una de las interpretaciones más utilizadas en el análisis de riesgo de activos digitales es que el valor del riesgo se calcula por el daño que pueda generar en el activo. Sin embargo, para las pequeñas empresas que cuentan con limitados recursos y buscan oportunidades de negocio mucho más grandes que su activos, el verdadero valor del riesgo radica en la oportunidad de negocio que se puede perder y no en el daño del activo mismo.

Un modelo ágil no debe preocuparse por la probabilidad de que a un activo le suceda un evento inesperado o no, sino de que ocurra durante uno de los procesos de la organización; e igualmente no debe importarle la repercusión que tenga sobre el activo sino la incidencia que su daño tenga sobre los procesos de la empresa.

Tabla 9
Porcentaje de riesgos primarios detectados

PORCENTAJE DE RIESGOS PRIMARIOS DETECTADOS				
MADUREZ DEL SISTEMA ORGANIZACIONAL	DIMENSIÓN DEL SISTEMA ORGANIZACIONAL			
		EP	EM	EG
	EPM	80% a 100%	40% a 70%	20% a 60%
	EMM	40% a 70%	20% a 60%	10% a 40%
	EGM	20% a 60%	10% a 40%	0% a 20%

Tabla 10
Porcentaje de conocimiento agregado sobre amenazas descubiertas

PORCENTAJE DE CONOCIMIENTO AGREGADO SOBRE AMENAZAS DESCUBIERTAS				
MADUREZ DEL SISTEMA ORGANIZACIONAL	DIMENSIÓN DEL SISTEMA ORGANIZACIONAL			
		EP	EM	EG
	EPM	70% a 100%	80% a 70%	90% a 100%
	EMM	40% a 60%	30% a 80%	20% a 90%
	EGM	0% a 20%	0% a 30%	0% a 40%

Tabla 11
Resultados de eficiencia

TIEMPO DE ANÁLISIS PROMEDIO POR PROCESO				
MADUREZ DEL SISTEMA ORGANIZACIONAL	DIMENSIÓN DEL SISTEMA ORGANIZACIONAL			
		EP	EM	EG
	EPM	6 horas	13 horas	30 horas
	EMM	1.5 horas	3 horas	6 horas
	EGM	50 minutos	1.5 horas	3 horas

Tabla 12
Resultados de eficiencia

TIEMPO DE ANÁLISIS PROMEDIO POR ACTIVO				
MADUREZ DEL SISTEMA ORGANIZACIONAL	DIMENSIÓN DEL SISTEMA ORGANIZACIONAL			
		EP	EM	EG
	EPM	De 3 a 6 horas	De 10 a 13 horas	De 15 a 20 horas
	EMM	De 1 a 2 horas	De 1.5 a 3 horas	De 2 a 5 horas
	EGM	De 15 a 30 minutos	De 45 a 90 minutos	De 1 a 2 horas

Bibliografía

– MERCHÁN, Luis (2010). *Planificación de proyectos de mejoramiento. Un enfoque a las pequeñas empresas de programa*. Cali: Editorial Faribe.

– INTERNATIONAL ORGANIZATION FOR STANDARDIZATION.*ISO/IEC 27001: Seguridad de la información*. Publicado en la red. Consultado el 23 de noviembre de 2009.

– HILLSON,David. SIMON, Peter (2007). *Practical Project Risk Management. The Atom Methodology*. Vienna, Virginia. Inc

– ALEXANDER, Alberto (2007). *Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005*. México: Alfaomega.

– BS 7799. *The BS 799 Security Standards*. http://www.riskserver.co.uk/bs7799/. Publicado en la red. Consultado el 12 de agosto de 2009.

– INTERNATIONAL ORGANIZATION FOR STANDARDIZATION.*ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management.*http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm. Publicado en la red. Consultado el 16 de agosto de 2009.

– NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY -NIST.*Risk Management Guide for Information Technology Systems*.http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. Publicado en la red. Consultado el 22 de noviembre de 2009.

– INTERNATIONAL ORGANIZATION FOR STANDARDIZATION- ISO.http://SC27N5716_SD6_Glossary_IT security_Apr2007.ZIP. Publicado en la red. Consultado el 23 de agosto de 2007.

– Margerit (1997). *CASE. Proyecto Margerit Versión 2.*<http://www.csi.map.es/csi/pdf/magerit_v2/>. Publicado en la red . Consultado el 17 de julio de 2009.

– NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY-NIST.*A guide to security management for it systems draft Managing Risk from Information Systems: An Organizational Perspective.*http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf. Publicado en la red. Consultado el 5 de abril de 2009.

– FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 199. *Standards for Security Categorization of Federal Information and Information Systems.http://csrc.nist.gov/publications/fips/index.html.* Publicado en la red. Consultado el 25 de septiembre de 2009.

– NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY-NIST.*SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.* http://csrc.nist.gov/publications/nistpubs/index.html. Publicado en la red. Consultado el 23 de septiembre de 2009.