Enfoque UTE, V.7-Sup.1, Feb.2017, pp.107 - 121
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542 / p-ISSN: 1390-9363
Recibido (Received): 2017/01/09
Aceptado (Accepted): 2017/02/24

Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs

(ECU@Risk, a methodology for risk management applied to MSMEs)

Esteban Crespo Martínez[1]

Resumen:
La información es el elemento más valioso para cualquier organización o persona en este nuevo siglo, la cual, para muchas de ellas, es un instrumento para crear ventaja competitiva (Vásquez & Gabalán, 2015). Sin embargo, pese a la falta de conocimiento sobre cómo protegerla adecuadamente, o a la complejidad de las normas internacionales que indican los procedimientos para lograr un adecuado nivel de protección, muchas organizaciones, en especial el sector MPYME, no logra alcanzar este objetivo.
Por lo tanto, este estudio propone una metodología de seguridad de la información para la gestión del riesgo informático aplicable al entorno empresarial y organizacional del sector MPYME ecuatoriano. Para el efecto, se analizan comparativamente varias metodologías de amplia divulgación, como: Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III. Estas metodologías son internacionalmente utilizadas en la gestión del riesgo de información; a la luz de los marcos de referencia de la industria: ISO 27001, 27002, 27005 y 31000.

Palabras clave: riesgos, gestión, ECU@Risk, Seguridad de la Información.

Abstract:
Information is the most valuable element for any organization or person in this new century, which, for many companies, is a competitive advantage asset (Vásquez & Gabalán, 2015). However, despite the lack of knowledge about how to protect it properly or the complexity of international standards that indicate procedures to achieve an adequate level of protection, many organizations, especially the MSMEs sector, fails to achieve this goal.
Therefore, this study proposes a methodology for information security risk management, which is applicable to the business and organizational environment of the Ecuadorian MSME sector. For this purpose, we analyze several methodologies as Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 COSO III. These methodologies are internationally used in risk management of information; in the light of the frameworks of the industry: ISO 27001, 27002, 27005 and 31000.

Keywords: Risk, management, ECU@Risk, Information Security.

[1] Universidad del Azuay, Cuenca – Ecuador (ecrespo@uazuay.edu.ec)

1. Introducción

Desde tiempos inmemoriales, tener la información justa en el momento oportuno ha significado 'poder' y solamente las personas o grupos de personas que se podían permitir financiar ese intercambio de información disfrutaron de ese privilegio. Si partimos de un concepto generalmente aceptado de que "la información es poder", frase que se atribuye a Francis Bacon- quien posee la capacidad de control no es quien sabe dónde encontrar determinado dato, antecedente, fuente o material, sino más bien quien sabe cómo usar aquello que encontró. Esto genera la búsqueda de habilidades para manejar la información, muchas veces para aprovecharse de ella, con diversas motivaciones, muchas veces con fines de tendencia negativa, generando riesgo con diferentes niveles de impacto por lo que es crucial protegerla pues constituye uno de los activos más importantes de una organización.

Para efecto de su gestión en las organizaciones, se emplea el concepto de Inteligencia de Negocios, un conjunto de herramientas y servicios que permiten a los usuarios acceder y analizar de manera rápida y sencilla, a la información para la toma de decisiones de negocio a nivel operativo, táctico y estratégico; considerando: que los datos son elementos constitutivos del conocimiento, que la información es una interpretación de ellos basada en un cambio de las condiciones y en el paso del tiempo, la que incluye patrones, relaciones y significado a los datos y que el conocimiento: es la información organizada dentro de un marco conceptual que nos permite comprender nuestro entorno, mejorar la capacidad para resolver problemas y tomar decisiones. Consecuentemente su desarrollo se transforma en un activo de alto valor implícito y explicito que incide en la economía de una organización por lo que se requieren niveles adecuados para su protección.

La Seguridad de la Información se basa en tres principios fundamentales: i) la integridad que hace referencia a que la información debe estar libre de alteraciones o modificaciones no planificadas (Gómez, 2011), ii) la disponibilidad que indica que la información debe ser utilizable cuando se la requiera (Gómez, 2011), y iii) la confidencial porque solo debe ser accedida por los que lo requieren (Gómez, 2011). La mala administración, o la carencia de un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización, puede conllevar a un efecto llamado riesgo operativo (Calderón, Estrella, & Flores, 2011).

El riesgo operativo consiste en la posibilidad de que se produzcan pérdidas debido a los eventos originados, ya sea por fallas en procesos, personas, sistemas internos, tecnología, o por eventos externos imprevistos (Superintendencia de Bancos y Seguros, 2011), por lo que el acceso a la información deberá ser correctamente controlado, otorgando permisos a quienes tengan autorización de los propietarios de la información. Consecuentemente se requiere de una adecuada gestión de los perfiles de usuario y el acceso a la misma.

Mediante un proceso de indagación exploratoria realizada, no se ubica organización, institución o empresa ecuatoriana que haya emprendido en la tarea del desarrollo de una metodología para la gestión del Riesgo de Información que considere la realidad nacional en el entorno MPYME. Las Instituciones de control se han limitado a solicitar la implementación de prácticas internacionales, que muchas veces ni las grandes empresas logran cumplir, debido a la cantidad de parámetros y procedimientos exigidos por las normas.

Las MPYMES, en general, están inmersas en un eminente entorno de riesgo, ya sea a nivel nacional por la inestabilidad política y/o económica; o regional debido a las condiciones naturales en las que se asienta cada ciudad, a más de que consideran que la informática es solamente un área de soporte, y que la inversión en elementos y mecanismos de seguridad convergen solamente en una solución antivirus. El desconocimiento, la exigencia y extensión de las normas, ayudan a que el concepto de gestión de riesgo informático quede como un mito empresarial. Con la finalidad de comprobar esta hipótesis, y, como validación, se realizó, mediante el modelo cualitativo de investigación por conveniencia, un estudio a 50 empresas del sector MPYME en este país, obteniendo como resultado que, muy pocas gestionan el riesgo de información, y aquellas que lo hacen, la desarrollan, de forma elemental.

Como comprobación adicional se procede a la caracterización de las MPYMES de la región austral del Ecuador en relación con las TI y la seguridad de la información, para obtener una base coherente que permita, a este trabajo de investigación, como objetivo, proponer una metodología para la Gestión del Riesgo Informático, que consienta aplicarse, inicialmente, al entorno ecuatoriano, proporcionando directrices para i) identificar el contexto organizacional, ii) identificar y registrar los activos de información, iii) identificar y valorar los riesgos y amenazas físicas, de entorno, y lógicas, iv) directrices para el desarrollo de contramedidas y políticas de seguridad.

Para efecto de una adecuada sustentación teórica, fue importante realizar el análisis comparativo entre las metodologías Magerit V3, Microsoft Risk Management, Octave-S y CRAMM, metodologías internacionales utilizadas en el análisis y gestión de riesgo informático, en base a mecanismos de identificación de activos, identificación de vulnerabilidades, funciones de probabilidad, variable de medición de riesgo, y cálculo de riesgo; además de incluir un estudio de los aspectos de regulación local, nacional, internacional y las normas que tratan el riesgo; agregando además, el estudio de los marcos de gestión COBIT 5 y COSO III, y las normas internacionales ISO 27001, ISO 27002, ISO 27003, e ISO 27005.

Considerando que todos estos elementos permiten la realización de una adecuada investigación y propuesta de solución, se la ha organizado de la siguiente manera:

1. el apartado dos verifica la metodología utilizada en la investigación haciendo referencia al análisis de la situación actual de las MPYMEs en el Ecuador en relación al riesgo informático,

2. en la sección tres se presentan los resultados obtenidos a la investigación aplicada a las MPYMEs analizadas,
3. en el apartado cuatro, como tema principal, se explica la metodología Ecu@RISK, como propuesta de una herramienta para la gestión del riesgo de información,
4. en el apartado cinco se expone la discusión a esta investigación,
5. en el apartado seis, se incluyen las conclusiones y trabajos futuros,
6. en el apartado siete se considera la bibliografía utilizada en este trabajo.

2. Metodología

Partiendo de lo conceptual, el término MPYME hace referencia a las micro, pequeñas y medianas empresas, concepto que según Vásquez y López (Vásquez & López, 2016), citando a Muñoz (Muñoz, 2012), en el Ecuador está clasificado de la siguiente manera:

> 1. La microempresa, que es una entidad con escasos ingresos y está compuesta por un número de empleados igual o menor a 10 personas, con un volumen anual de negocio que no supera los 20 mil dólares (Vásquez & López, 2016).
>
> 2. La pequeña empresa, que es una entidad independiente, creada para generar rentabilidad, con un número de empleados inferior a 50 personas y con volúmenes entre los 20 mil y 120 mil dólares (Vásquez & López, 2016).
>
> 3. La mediana Empresa, caracterizada por el capital suministrado por sus propietarios, y un tamaño relativamente pequeño dentro del sector en el que se desarrolla, albergando entre 50 a 99 empleados, y su capital fijo no sobrepasa los 120 mil dólares (Vásquez & López, 2016).

En una rueda de prensa, el especialista de seguridad informática, Dimitry Bestuzhev mencionó que “A pesar de que se han hecho esfuerzos, en Ecuador, todavía no se trabaja en seguridad de manera sistemática con políticas definidas. El Gobierno no tiene un plan de acciones para todas las entidades del país. Muchas veces es el propietario o el administrador del sitio web el que decide qué hacer para que este sea seguro, por ello Ecuador llega a ser un blanco fácil de los atacantes.” (Delgado, 2014).

La ley Orgánica de transparencia y acceso a la información pública, según (Jaramillo Palacios, 2014), garantiza el derecho de acceder a las fuentes de información, además de ser un mecanismo para ejercer la participación democrática respecto del manejo de la cosa pública y la redición de cuentas, y que la información confidencial está excluida del principio de publicidad. También menciona sobre la creación de. la Ley del Sistema Nacional de Registro de Datos Públicos - SINARDAP, cuya finalidad es proteger los derechos constituidos, además de regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica, el comercio electrónico, y la protección a los usuarios de estos sistemas.

Entidades de control como la Superintendencia de Bancos y Seguros a través de sus disposiciones, han definido resoluciones que exigen un control en la calidad de información, confiabilidad en la ejecución de transacciones, y políticas y procedimientos para el monitoreo de los niveles de seguridad en hardware, software y redes de comunicaciones; lo que claramente evidencia la preocupación por integrar e incorporar mecanismos que protejan la información confidencial de los clientes, que muchas veces es accedida por el personal de desarrollo de sistemas, elevando el riesgo de manipulación o hurto de la misma; agregando además que se debe dejar evidencia de cualquier acceso o modificación a la información, lo que conlleva a que la metodología para la gestión de riesgos a proponer, considere aspectos que permitan a las entidades de control, evaluar los procedimientos y actividades contempladas en la misma; o bien, estar alineada a una metodología internacional como COBIT, que, entre uno de sus dominios, permite lograr este objetivo.

Una metodología debe estar enmarcada en un referente legal. En Ecuador, la Ley Orgánica de Protección de Datos establece que se garantizará el derecho de protección de los datos personales y su gestión. Los datos personales deben ser correctos, completos, actualizados y relevantes, para la actividad en la cual serán utilizados (García Falconí, 2011).

Para determinar la situación de las empresas frente al riesgo, se ha empleado el método no probabilístico de muestreo por conveniencia, que se trata de una técnica de tipo cualitativo donde los sujetos son seleccionados dada la conveniente accesibilidad y proximidad de los sujetos para el investigador, y que eS comúnmente utilizada mediante la selección de una muestra de una población que sea accesible, es decir, que se seleccionan porque están fácilmente disponibles y no necesariamente que se lo efectúe bajo un criterio estadístico que considere un método probabilístico de orden cuantitativo; lo que posibilita la generalización a sujetos similares (Bernal, 2006). Así, se ha considerado el siguiente grupo MPYME, en un estudio realizado a 50 instituciones de este sector donde el autor de este trabajo tiene acceso, las mismas que se encuentran distribuidas según lo enseña la *Figura 1*:

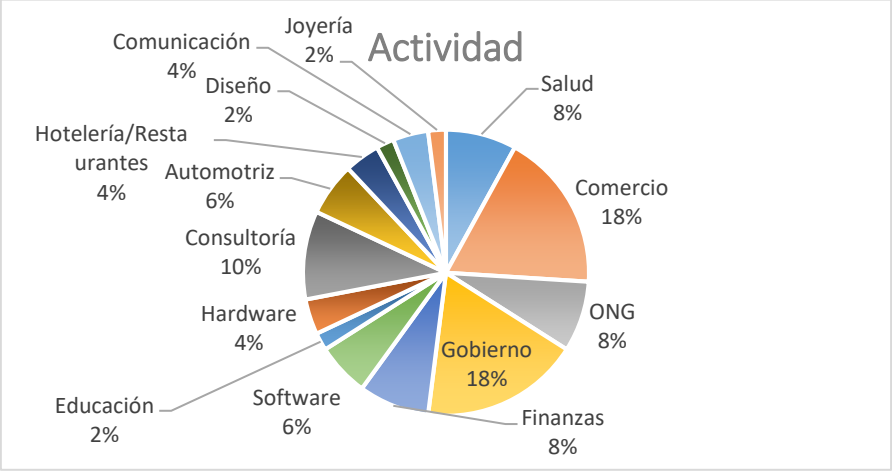

Figura 1: Sector de actividad económica. Fuente: Resultado de la Investigación.

Para la muestra por conveniencia se han tomado como criterio principal, la localidad, la capacidad de gestión, tamaño e importancia de la unidad productiva y la significación de su magnitud de riesgos en términos de importancia y magnitud de operaciones (Bernal, 2006).

3. Resultados

En la aplicación de las herramientas muestrales, una de las preguntas realizadas estuvo relacionada con el mantener un inventario de los activos de información. Solo un 4% de los entrevistados sostuvieron que cuentan con un inventario de los activos de información, aunque no se encuentra del todo actualizado.

Las razones por las que las empresas que no cuentan con un plan de gestión de riesgo formal, representadas en la *Figura 2*, se resumen en el desconocimiento del proceso de gestión de riesgos, en la falta de presupuesto, y en la complejidad que presentan las normas ISO.

Figura 2: Razones por las que no se adopta un modelo de gestión de riesgo de información

El 100% cuenta con prácticas de respaldo de información, sin embargo, solo un 42% los realiza bajo procedimientos formales, y únicamente el 24% de las organizaciones del sector MPYME tienen identificadas, formalmente, las áreas físicas sensibles; es decir, espacios en los que la información debe ser gestionada con niveles de seguridad superiores.

En cuanto a planes para protección de los recursos humanos, se puede evidenciar que no existen procedimientos formales para llevar a cabo la evacuación de un edificio en caso de un incidente. Así, solamente un 14% de los entrevistados saben, formalmente, que hacer. (Crespo, 2016)

Los análisis de estos y otros elementos permiten determinar una falencia real que no está siendo cubierta en relación con el riesgo de información, lo que nos lleva a pensar en la validez de la hipótesis planteada en el sentido de que ECU@Risk, puede constituir una metodología adecuada para el sector MYPYME.

4. ECU@Risk

ECU@Risk, como se ha llamado a la metodología para la gestión de riesgo de información enfocada a las MPYMES, contempla 4 dominios, representados en la *Figura 3*.

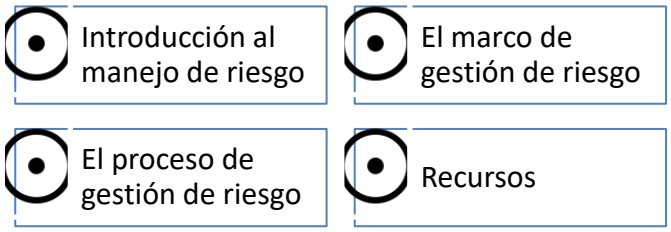

Figura 1: Los dominios de ECU@Risk

ECU@Risk parte de una necesidad clave: Las organizaciones MPYMES ecuatorianas no están preparadas, o aún mantienen niveles iniciales en cuanto a gestión de riesgo se refiere.

Esta metodología propuesta está basada en los principios de la administración de riesgos, provista por los estándares ISO 31000:2009, y en las mejores prácticas de seguridad de la información: ISO 27001, ISO 27002 e ISO 27005, además del estudio de las principales metodologías internacionales usadas para la gestión de riesgos y seguridad de la información. La metodología se resume en un manual, el mismo que brinda los procesos mínimos requeridos para gestionar de forma adecuada la información de una organización.

Al saber que una MPYME también es influenciada por factores exógenos, como los cambios políticos (entorno externo), cambios de gobierno corporativo (entorno interno), recortes presupuestales, inestabilidad de la economía global, riesgos monetarios, sostenibilidad financiera y uso de recursos limitados; globalización y la revolución digital, productos sustitutos, tendencias, moda; el alto costo de equipamiento tecnológico, y el intenso escrutinio de las instituciones de control, hacen que la organización descuide sus procesos de gestión de riesgo, o que simplemente no los adopte.

Así, ECU@Risk sugiere los roles y responsabilidades del personal que debe soportar y participar en los procesos de gestión, en los que se menciona la alta dirección, los propietarios de la información, los propietarios de los sistemas de información, un comité de riesgo de TI, el coordinador de seguridad designado, los profesionales de TI, y un comité de certificación de productos y servicios de TI.

Esta metodología considera el ciclo de un Sistema para la gestión de riesgos, el mismo que consiste en cuatro etapas: i) Planificar, ii) Ejecutar, iii) Verificar y iv) Actuar; conformando 5 procesos de gestión, un proceso de monitoreo y control, y un proceso comunicacional. A continuación, se detalla cada uno de ellos.

Establecer el contexto

Este primer paso cuenta con los procedimientos necesarios para identificar el tipo y tamaño de organización; que permitirán definir el alcance de la investigación y sus objetivos; e identificar los interesados y/o áreas pertinentes involucradas o afectadas, así como los factores internos y el ambiente externo.

En este primer proceso, se han considerado los siguientes subprocesos:

1. Procedimiento para el tipo y tamaño de organización, considerando las políticas del Servicio de Rentas Internas ecuatoriano.
2. Procedimiento para la identificación del contexto externo, considerando la herramienta PESTEL (Político, Económico, Social, Tecnológico, Ecológico y Legal)
3. Identificación del contexto interno, en base al análisis EFI soportado en la matriz FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)
4. Identificación del contexto interno, utilizando la herramienta de las 7S de McKinsey.

Identificar los activos de información

Los activos de información, en una organización, hacen referencia a cualquier elemento que contenga información. ECU@Risk plantea los siguientes grupos de clasificación de activos de información que deberán ser considerados:

(ED) Edificaciones, (HW) Hardware, (SW) Software, (IE) Información Electrónica, (IP) Información en Papel, (Extraíble) Medios de almacenamiento extraíbles, (IC) Infraestructura de comunicaciones, y (RRHH) Recursos Humanos.

Para lograr esta clasificación, se propone considerar los siguientes sub procesos:

1. Identificar los activos de información, para lo cual proporciona procedimientos y herramientas que apoyen a esta clasificación, acotando que es importante considerar que la codificación del activo de información debe contener: (COD. CLASIFICACIÓN DEL ACTIVO) (SUB CODIGO) (SUB CÓDIGO) (SECUENCIAL), donde el campo secuencial es un número incremental, que permite distinguir a un activo de información frente a otro.
2. Una vez identificados los activos de información, será necesario valorarlos. Para ello, la metodología sugiere realizar esta valoración según criterios de confidencialidad, integridad y disponibilidad, agregando que, para este efecto, se puede utilizar cualquier escala. ECU@Risk sugiere una escala de diez niveles, donde 0 es despreciable y 10 es extremo.

Identificar los riesgos

Para esta secuencia de pasos, se ha sugerido partir de las siguientes premisas:

- ¿Qué puede pasar?

- ¿Cómo puede pasar?
- ¿Dónde puede suceder?
- ¿Por qué podría suceder?
- ¿Cuál podría ser el impacto si se presenta el riesgo?
- ¿Cuál podría ser el impacto si se materializa el riesgo?

Los subprocesos que se han considerado en esta etapa consisten en:

Identificación de amenazas, para lo cual se proporcionan formatos y lineamientos para su correcta identificación.

Valoración de amenazas, en base a criterios de impacto. Para ello, se proporciona la forma de hacerlo en la metodología.

En Ecuador, las amenazas que pueden afectar a las operaciones de una organización se clasifican de acuerdo a lo expuesto en la *Figura 4*:

Figura 2: Clasificación de los riesgos organizacionales en Ecuador

Analizar los riesgos

Una vez que el riesgo ha sido identificado, el contexto, causas, factores de contribución y las consecuencias que han sido descritas, se deben considerar las fortalezas y debilidades de los sistemas y procesos designados para ayudar a controlar el riesgo. Debe conocerse cuales controles ya se encuentran identificados e implementados, si estos son eficaces, si contribuyen en la identificación de algo, si es necesario seguir actuando, o simplemente no colaboran con ninguna acción.

Para ello, este proceso considera el siguiente sub proceso:

> Análisis del Riesgo: Para ello, proporciona mecanismos para identificar los controles existentes, la evaluación de probabilidad de ocurrencia, la evaluación de la consecuencia,

la valoración del nivel de riesgo, todos ellos en 5 niveles. Para esta valoración, se sugiere hacer referencia a la *Tabla 1*.

Tabla 1: Matriz de riesgos

Matriz de Riesgos						
		Consecuencia				
		1. Leve	2. Menor	3. Moderado	4. Alto	5. Extremo
Probabilidad	E - Casi cierto (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Evaluar los riesgos

Este proceso proporciona directrices para decidir si los riesgos son aceptables o inaceptables. Lo comprendido sobre el riesgo, se lo utiliza para tomar decisiones acerca de acciones futuras. Estas decisiones deben incluir:

1. No emprender o continuar con el evento, actividad, proyecto o iniciativa.
2. Tratar activamente el riesgo.
3. Priorizar las acciones necesarias.
4. Aceptar el riesgo.

Tratar los riesgos

De los resultados obtenidos en la matriz de Riesgo, se deberán considerar los niveles de aceptación de riesgo, sugeridos en la *Tabla 2*:

Tabla 2: Niveles de riesgo

Niveles de riesgo - Acción de gestión requerida	
Riesgo extremo (E)	Requiere respuesta y atención inmediata.
Riesgo alto (A)	Debe otorgársele la atención apropiada.
Riesgo medio (M)	Evaluar el riesgo y determinar si los controles implementados son suficientes y si están siendo efectivos.
Riesgo Bajo (B)	Administrar mediante procedimientos rutinarios; informar a los gestores locales; supervisar y revisar localmente como sea necesario.
Riesgo Leve (L)	Monitoreo constante a las actividades diarias. Registrar eventos en bitácora.

Para tratar los riesgos de manera adecuada, la metodología sugiere los siguientes aspectos:

1. Decidir si es necesario un tratamiento específico o si el riesgo puede ser tratado adecuadamente durante el curso de procedimientos normalizados de gestión y actividades de tratamiento específico.

2. Trabajar en lo que se quiere como deseable para el tratamiento de riesgo.
3. Identificar y diseñar una opción preferente de tratamiento, una vez que el objetivo del tratamiento ha sido conocido.
4. Evaluar las opciones de tratamiento y su viabilidad en relación con la tolerancia al riesgo.
5. Documentar el plan de tratamiento de riesgo.
6. Aplicar los tratamientos acordados.
7. Consideraciones para evaluar el riesgo residual, una vez que todos los riesgos hayan sido tratados.

Identificar las contramedidas

Para seleccionar las contramedidas que brindarán protección a los activos organizacionales, se considerará, primeramente, los elementos de protección actual establecidos, y luego los posibles elementos de control que podrán ser implementados. Este procedimiento hace referencia a los elementos de salvaguardas que deben considerarse como contramedidas que permitan gestionar los riesgos, sugeridos en la *Tabla 3*.

Tabla 3: Tipo de protección

TIPO DE PROTECCIÓN	
PGeneral	Protección de tipo general
PInfo	Protección de Información Electrónica y de Papel
PSW	Protección de software
PHW	Protección del hardware
PIC	Protección de la Infraestructura de Comunicaciones
PSF	Seguridad Física, relativa a edificaciones e instalaciones.
PRRHH	Relativas a los Recursos Humanos

Monitorear y Revisar

Esta etapa hace referencia a la supervisión de cambios en la fuente y el contexto de los riesgos, la tolerancia a ciertos riesgos y la adecuación de los controles. Busca garantizar que los procesos se encuentran implementados para revisar, evaluar e informar sobre los riesgos con regularidad.

Como procedimientos, la metodología considera:

Monitoreo continuo, mediante una política de reporte y monitoreo, en el que los actores fundamentales son el Comité de Riesgos y Auditoría interna.

Reportar formalmente, donde la organización se somete a la obligación de informar a cada uno de los interesados (stakeholders) de manera oportuna y transparente.

Consideraciones al momento de registrar, como, por ejemplo, las causas, consecuencias y controles actuales.

Comunicar y consultar

La comunicación efectiva y la consulta son esenciales para asegurar que los responsables de la implementación de la gestión de riesgos, y los que tienen un interés personal, puedan comprender la base sobre la que se toman las decisiones y las razones por las cuales se seleccionan las opciones de tratamiento particulares. Para ello, se sugiere incluir:

1. Reuniones
2. Reportes
3. Sistemas de comunicación en línea
4. Talleres de inducción y capacitación a los empleados
5. Noticias
6. Grupos focales

La última sección del documento hace referencia a los recursos, que incluye las matrices sugeridas para la identificación de los activos de información, la matriz para la gestión de riesgos, la matriz para el registro y cálculo de riesgos, la matriz para el manejo de riesgos y un cuestionario sugerido para la aplicabilidad de la metodología.

ECU@Risk cuenta con una proyección hacia COBIT 5 y COSO III, debido a que incluye aspectos relacionados con la identificación del contexto organizacional, la evaluación de los aspectos que conlleven a fraudes, la identificación de las actividades de control (establecimiento de contramedidas) (Minchala, 2016), procedimientos para el monitoreo continuo y métodos para reportar a los interesados; considerando Principios, políticas y modelos de referencia, procesos, estructuras organizacionales, cultura, ética y comportamiento, información, servicios, infraestructura y aplicaciones, gente, habilidades y competencias (Delgado, 2014) .

5. Discusión

Considerando que la información es uno de los activos más valiosos de una organización y que su protección es de suma importancia, proponer un modelo de gestión para la seguridad de la información, basado en las mejores prácticas y métodos existentes, tendiente a facilitar su implementación y uso en las MYPYMES nos llevó a diseñar un modelo particularizado.

La metodología propuesta resume las mejores prácticas de las normas internacionales ISO 27001, ISO 27002, ISO 27005 e ISO 31000; además de las metodologías Magerit V3, Microsoft Risk Management, Octave-S y CRAMM, la proyección a los marcos de referencia COBIT 5 y COSO III, así como también múltiples herramientas de las ciencias administrativas, todo esto considerando el estudio del marco legal ecuatoriano.

Al sintetizar y extraer la esencia de cada uno de los estudios anteriores se ha logrado la construcción de una metodología que pueda aplicarse en un contexto MPYME, considerando que, las organizaciones de este sector cuentan con recursos limitados.

El desconocimiento, la confianza con los empleados y los proveedores, la cantidad de exigencias que forman parte de las ISO, la complejidad de los marcos de referencia, y las leyes ambiguas que atienden el tratamiento de la información en el Ecuador, conllevan a que las empresas de este sector desistan en la adopción de mecanismos formales para el tratamiento de riesgo.

Se espera que ECU@Risk aporte a esta complicación que mantienen las MPYMES, debido a que las herramientas que se incluyen en esta metodología son de fácil utilización, considerando todas y cada una de las etapas que requiere la gestión de riesgos; eso es, la identificación del contexto organizacional, la identificación y valoración de los activos de información, la identificación y valoración de las amenazas y su frecuencia de ocurrencia, la ponderación del riesgo, la identificación de contramedidas y el tratamiento del riesgo residual.

Finalmente, se puede acotar que, si bien se ha realizado una prueba concepto dentro de las instituciones, las próximas actividades a realizar consistirán en aplicar la metodología en diferentes instituciones del sector MPYME, a manera de evaluar la efectividad de la misma y proceder con los ajustes necesarios; al mismo tiempo que permitirá que este tipo de organizaciones adopten prácticas puntuales y alcanzables en cuanto a la gestión de riesgo de información se refiere.

6. Conclusiones y Recomendaciones

Es posible que varios negocios y organizaciones situadas en la costa ecuatoriana, luego de la tragedia provocada por el terremoto del 2016, hayan perdido su información o retomado las operaciones luego de un tiempo considerable, a causa de la carencia de un plan de continuidad. Es interesante cuestionarse ¿Qué pasó con la información de inventarios o de facturación que mantenían esas MPYMES? ¿Cómo saber cuáles son sus deudores y cuál es el valor a cancelar a sus acreedores? Es probable que los activos físicos se hayan visto afectados, pero en sí la información debería ser recuperada si se contaba con un adecuado plan de contingencia y procedimientos claros para la gestión de riesgos. Está claro que las empresas del sector MPYME no están preparadas para enfrentar los riesgos de manera formal, esto es, los riesgos son manejados a un nivel AdHoc o simplemente los maneja como respuesta a un incidente. De esta manera se puede concluir que:

1. La retroalimentación de cada una de las metodologías estudiadas ha permitido asimilar las mejores cualidades y características de cada una, en las que se ha podido comprobar que la gestión de riesgos se resume en la identificación y valoración de los activos de información, la identificación y valoración de amenazas, el cálculo de riesgos, la identificación de contramedidas y el manejo del riesgo residual; recalcando que cada una de ellas adopta las mejores prácticas de las ISO27001, 27002, 27005 y 31000; utilizadas para la gestión de la seguridad de la información y la gestión del riesgo.

2. ECU@Risk es una metodología fruto del análisis de otras múltiples utilizadas a nivel internacional para la gestión de riesgos, las mismas que reflejan aspectos positivos y consideraciones especiales de cada una de las normativas ISO utilizadas para este propósito; integra además múltiples herramientas propias de la gestión empresarial, tales como el PESTEL, las 7S de McKinsey o el FODA. Además, propone una plantilla que servirá para la recolección y valoración de cada uno de los datos relevantes que componen un activo de información, sabiendo que estas ayudarán a inventariarlos, estudiarlos, administrarlos y gestionarlos.
3. ECU@Risk propone procesos para el inventario de activos de información, considerando como categorías principales i) edificaciones o instalaciones, ii) el hardware, iii) el software, iv) la información electrónica, v) la información en papel, vi) la infraestructura de comunicaciones, vii) los medios de almacenamiento extraíbles y viii) los recursos humanos; elementos con que toda organización del sector MPYME cuenta.
4. Tal como lo establece COBIT, ECU@Risk analiza aspectos relacionados con las estructuras organizativas, donde para cada empresa tendrá definida una estructura variada; y que, en función de su composición y ámbito de decisiones, las mismas podrán ubicarse en el área de gobierno o en el de gestión.
5. ECU@Risk está alineada a la normativa vigente, en la que se ha considerado el análisis de los aspectos legales, partiendo del estudio de regulaciones internacionales y compararla con las leyes ecuatorianas, en las que se ha podido ver, de manera inicial, un bajo nivel de madurez en estas últimas. Las acciones que ECU@Risk considera en sus todos sus procesos son legales, pues se encuentran dentro del marco normativo vigente y no a la voluntad de cada persona, tema que fue discutido por Jaramillo Palacios en el 2014 (García Falconí, 2011). Además, cumple con la “calidad de los textos normativos”, ya que incluye procedimientos claros que no van contra de la Constitución de la República del Ecuador. ECU@Risk puede ser de interés público y estar disponible en formatos accesibles para los solicitantes e interesados en él, considerando siempre los derechos de propiedad intelectual.
6. Es vital que las MPYMES dentro de su marco legal organizacional considere crear conciencia a los usuarios y público en general; recolectar constantemente estadísticas y datos sobre incidentes informáticos, y registrarlos en bitácoras de control; establecer planes de capacitación continua al personal implicado en la seguridad de la información, además de una actualización permanentemente del marco normativo que contiene las políticas de seguridad de la información; y sobre todo la concienciación y compromiso de la alta gerencia.
7. Dentro del tratamiento de riesgos se han propuesto aspectos que deberían considerarse en la elección de contramedidas, conociendo que estas deberán ser alcanzables, aplicables, aceptables, además de medibles y registrables. Las políticas de seguridad

resultantes de la aplicación de esta metodología, aportarán a las decisiones de gobierno que deben ser sancionadas en la empresa.

8. Para que su aplicación sea efectiva en una MPYME, será importante la participación de la gerencia en los procesos de gestión de riesgo, pues el compromiso que mantenga es primordial para lograr mitigar los riesgos en conjunto con un buen equipo de trabajo y de esta manera alcanzar las metas y objetivos corporativos que se fusionan en una visión empresarial.

Bibliografía

Bernal, C. A. (2006). *Metodología de la Investigación.* México: Pearson Prentice Hall.

Calderón, D., Estrella, M., & Flores, M. (2011). Sistema de Gestión de Seguridad de la Información aplicada al área de recursos humanos de la empresa DECEVALE S.A. Guayaquil: Universidad Politécnica Salesiana.

Crespo, E. (2016). *Metodología de Seguridad de la Información para la gestión del Riesgo Informático aplicable a MPYMES.* Universidad de Cuenca, Cuenca.

Delgado, J. A. (2014). Ciberseguridad en Gobernanza de Internet en Ecuador: Infraestructura y acceso. *Encuentro Nacional de Gobernanza de Internet, Quito, Ecuador.* Quito.

García Falconí, J. (07 de 02 de 2011). *Revista judicial*. Obtenido de derechoecuador.com: http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2011/02/07/la-proteccion-de-datos-personales

Gómez, Á. (2011). *Enciclopedia de la seguridad informática.* México: Alfa-Omega.

ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Madrid: ISACA® Framework. doi:978-1-60420-282-3

Minchala, P. (2016). *Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI.* Universidad del Azuay, Cuenca, Ecuador.

Muñoz, D. C. (24 de Febrero de 2012). *dspace.* Obtenido de space: http://dspace.ups.edu.ec/bitstream/123456789/1442/5/Capitulo%202.pdf

Superintendencia de Bancos y Seguros. (2011). Gestión integral y control de riesgos. En *Normas generales para las instituciones del sistema de seguros privados* (págs. 95 - 107). Quito: Superintendencia de Bancos y Seguros.

Vásquez, F., & Gabalán, J. (2015). Información y ventaja competitiva. Coexistencia exitosa en las organizaciones de vanguardia. En *El profesional de la información* (págs. 149-156). Ebsco.

Vásquez, S., & López, D. (14 de 03 de 2016). Estudio comparativo entre las metodologías Microsoft Secure Risk Management y Octave. Cuenca, Azuay, Ecuador.