Ingeniería
ISSN: 0121-750X
revista_ing@udistrital.edu.co
Universidad Distrital Francisco José de Caldas
Colombia

Ramírez Castro, Alexandra; Ortiz Bayona, Zulima
Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios
Ingeniería, vol. 16, núm. 2, 2011, pp. 56-66
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia

Citación: Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: *Ingeniería, Vol. 16, No. 2, pág. 56-66.*

Artículo de Investigación

Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios

Technology risk management based on ISO 31000 and ISO 27005, and its contribution to business operation continuity

Alexandra Ramírez Castro
Ingeniera de Sistemas
Universidad Distrital Francisco José de Caldas
alexaramirezc@gmail.com

Zulima Ortiz Bayona
MSc. en Matemáticas
Miembro grupo de investigación Arquisoft, rama de Seguridad Informática, Universidad Distrital Francisco José de Caldas.
zortiz@udistrital.edu.co

Resumen

Este documento presenta una metodología para gestionar riesgos tecnológicos cuya base son los estándares ISO (International Organization for Standardization) 31000 e ISO/IEC (International Electrotechnical Commission) 27005, teniendo en cuenta que estos indican 'que' se requiere para la gestión de riesgos más no indican 'como' se puede realizar esta gestión. Además incluye recomendaciones y buenas prácticas de otros estándares y guías internacionales para manejo de riesgos, seguridad y gestión de servicios.

La metodología se desarrolla para riesgo tecnológico dado que el aumento en el uso de tecnologías de la información puede posibilitar puntos de quiebre o fisuras en aspectos de seguridad con respecto a su utilización, por ello se presenta una forma de aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde la perspectiva tecnológica. Como segunda parte se presenta una forma de integración de la metodología a la gestión de continuidad de negocios, como sustento al análisis de impacto sobre negocios y el desarrollo de estrategias en lo que respecta a procesos de base tecnológica.

Palabras clave: ISO 31000, ISO/IEC 27005, continuidad de negocios, riesgo tecnológico, seguridad de la información, tecnologías de la información.

Abstract

This document presents a methodology for technological risk management based on the ISO (International Organization for Standardization) 31000 and the ISO/IEC (International Electrotechnical Commission) 27005 standards, taking into account that in these, only the "what" is indicated (what is required for risk management) but they do not indicate the "how", (how to achieve such management). It also includes recommendations and best practices from other international standards and guidelines for risk management, security and services management.

The methodology was developed for technological risk given the increased use of information technology and hence the greater chance of breaking points or security holes arising during its use. Therefore it accounts for a form of assurance and control over the technology infrastructure (physical layer), information systems (logic layer) and organizational measures (human factor), from the technological perspective. The second part considers the integration of the methodology into the bussiness continuity management, giving support to the business impact analysis and strategies development in regards to technology-based processes.

Key words: business continuity, information security, information technologies, ISO 31000, ISO/IEC 27005, technological risks.

Fecha recibido: Junio 24/2011
Fecha modificado: Julio 24/2011
Fecha aceptado: Agosto 15/2011

1. Introducción

El uso de las tecnologías de la información (de ahora en adelante TI) se ha intensificado en las organizaciones independiente de la naturaleza y actividad de las mismas, estás se encuentran en constante evolución adaptándose a las nuevas necesidades de las organizaciones y así mismo dando lugar a otras relacionadas con su operación diaria. Adicionalmente su masificación las han convertido en blanco de ataques y vías para los mismos; los riesgos asociados a estas se intensifican y transforman y por ello se hace necesario crear y adaptar constantemente los medios y métodos utilizados para conservar la seguridad de la información que las organizaciones quieren proteger.

En este punto el desarrollo y uso de metodologías integradas y ágiles para gestionar riesgos y en especial el tecnológico es importante con el fin de minimizar el impacto que pueda causar la violación de alguna de las dimensiones de la seguridad (esto corresponde a la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad). Hasta el momento el marco existente para gestión de riesgos lo conforman los estándares ISO 31000 (*Risk management*) [3] e ISO/IEC 27005 (*Information security risk management*) [4]. Estos proveen lineamientos generales pero hace falta una guía más precisa que ofrezca pautas sobre *la forma* de lograr los aspectos de seguridad requeridos; adicionalmente este marco hace referencia a la gestión sobre los riesgos como concepto global y deja de lado el análisis de riesgos específicos como el tecnológico, lo más cercano es la administración del riesgo operativo en el que se relaciona de forma tangencial el riesgo tecnológico.

El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico. Una situación que ejemplifica lo mencionado ocurrió en la entidad financiera colombiana Bancolombia, en Febrero del año 2011; se presentó una caída de la red del banco lo cual produjo una suspensión en sus operaciones normales, que trajo como consecuencia caos en la atención a usuarios por aproximadamente una hora; lo anterior implicó pérdidas financieras significativas y afectación de la imagen para el banco [1].

Estos antecedentes motivaron el desarrollo de la metodología propuesta [2], que permite la gestión de riesgos de origen tecnológico cuya base son los estándares ISO 31000 [3] e ISO/IEC 27005 [4] de los cuales se realizaron las adaptaciones y especificaciones requeridas para este tipo de riesgo. Además se adoptaron e incorporaron recomendaciones y buenas prácticas de otras guías y metodologías para gestión de riesgos como MAGERIT [5], NIST SP 800-30 [6], NTC 5254 [7], ISO 27001[8] y lo correspondiente a seguridad en gestión de servicios de ITIL® v3 [9]. De igual forma se presenta una forma de ajustar esta metodología a la gestión de continuidad de negocios en lo respectivo a la definición de planes de gestión de incidentes tecnológicos.

2. Metodología para gestión de riesgo tecnológico

La metodología diseñada trabaja sobre procesos teniendo en cuenta que esto facilita el entendimiento sobre el funcionamiento de la organización y la definición de interacciones para la identificación de activos y riesgos asociados. Además, el analizar procesos permite

obtener una visión global de la organización y con ello el apoyo requerido por parte de la alta gerencia al mostrar la necesidad de proteger y gestionar procesos críticos de la organización. El trabajo sobre procesos no se debe entender como un trabajo aislado puesto que esta visión tiene en cuenta el factor humano que se encarga de su ejecución y desarrollo y toda la infraestructura que se requiere para su funcionamiento, lo anterior enmarcado dentro de los objetivos y estrategias organizacionales (ver Figura 1). De igual forma dentro del análisis de procesos se tienen en cuenta las actividades críticas que sustentan estos y a su vez sustentan la cadena de valor que permite ofrecer los productos y servicios de la organización. La gestión de riesgos tecnológicos aquí presentada tiene en cuenta la integración con los sistemas de gestión de la organización por ello su base es ISO 31000.

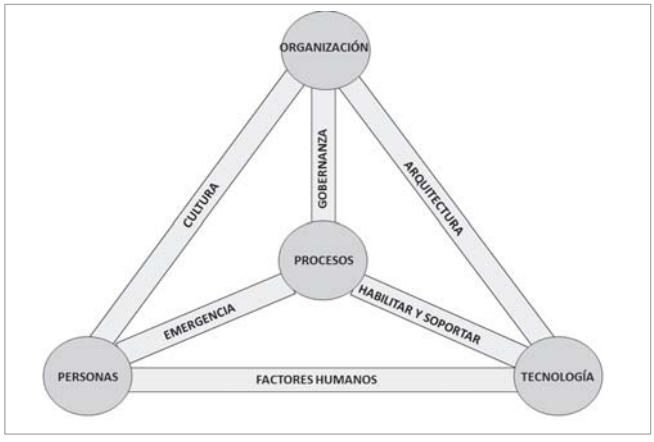

Figura 1. Modelo de negocio para seguridad de la información.
Fuente: Adaptación de: Institute for Critical Information Infrastructure Protection (ICIIP), University of Southern California Marshall School of Business, USA [13].

Esta metodología al tratar los lineamientos de la gestión de riesgos bajo el esquema presentado de organización integral, permite su inclusión en la gestión de continuidad de negocios como fase de apoyo, en lo respectivo a la identificación de dependencias claves, activos y procesos críticos, amenazas existentes y futuras. Erróneamente la gestión de continuidad es tomada como tratamiento de riesgos [10] pero es importante notar que esta última sirve de soporte para la definición de impactos que puedan producir no disponibilidad en la organización.

Un segundo punto de trabajo se relaciona con los activos de soporte a los procesos analizados. Se analiza hardware, software, recursos humanos y físicos. La finalidad de esta clasificación para el análisis es focalizar el estudio sobre los recursos críticos sin extenderse a activos irrelevantes (ver Figura 2).

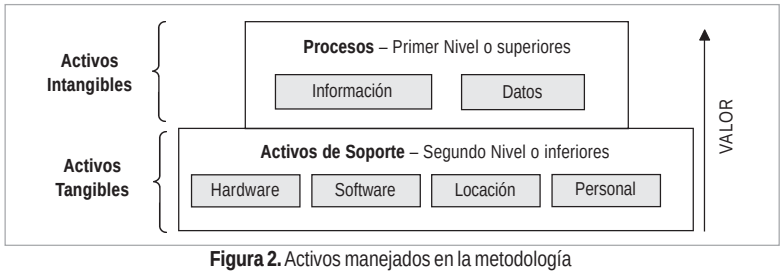

Figura 2. Activos manejados en la metodología

Para la metodología se utiliza como base el modelo PHVA [11] con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua siguiendo el esquema presentado a continuación:

PLANIFICAR: Se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Así mismo, se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos.

HACER: Corresponde a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la valoración y tratamiento de los riesgos.

VERIFICAR: Evaluar y medir el desempeño de los procesos contra la política y los objetivos de seguridad e informar sobre los resultados.

ACTUAR: Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye el monitoreo y mejora continua, donde se verifican los cambios y el cumplimientos de los indicadores que fueran establecidos desde la planificación.

Como se mencionó anteriormente, la metodología tiene su base en los estándares internacional ISO 31000 e ISO 27005, dado su enfoque en gestión de riesgos y siendo parte de los estándares de la familia ISO fue posible establecer una alineación entre los dos y ajustarlos a la metodología diseñada junto al modelo PHVA (ver Figura 3), a este marco fueron agregadas las mejoras provenientes de otras guías, entre ellas las que se mencionan a continuación:

<table>
<tr><th>PHVA</th><th colspan="3">ISO 27005</th><th colspan="2">ISO 31000</th></tr>
<tr><td rowspan="13">Planear</td><td colspan="3"></td><td colspan="2">Mandato y compromiso de la dirección</td></tr>
<tr><td colspan="3">Definir plan de gestión de riesgos</td><td colspan="2">Diseño del marco de trabajo para gestión riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td><td rowspan="12">Proceso de gestión del riesgo</td><td colspan="2">Entender la organización y su contexto</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Definir responsabilidades</td></tr>
<tr><td colspan="2">Recursos</td></tr>
<tr><td rowspan="3">Identificación del riesgo</td><td rowspan="3">Valoración Riesgo</td><td colspan="2">Integración con procesos</td></tr>
<tr><td colspan="2">Establecer mecanismo de comunicación</td></tr>
<tr><td rowspan="3"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="2"></td><td colspan="2">Establecer políticas para la gestión de riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td>Implementación del marco de trabajo para la gestión de riesgos</td><td>Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar plan de comunicación del riesgo</td><td colspan="2"></td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td><td colspan="2">Monitoreo y revisión del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td></tr>
</table>

Figura 3. Alineación de estándares ISO 31000 e ISO 27005 con modelo PHVA.

- NTC ISO/IEC 27001: Esta norma técnica colombiana especifica los requerimientos para implementación de controles de seguridad acordes con el planteamiento del sistema de gestión de seguridad de la información (SGSI).

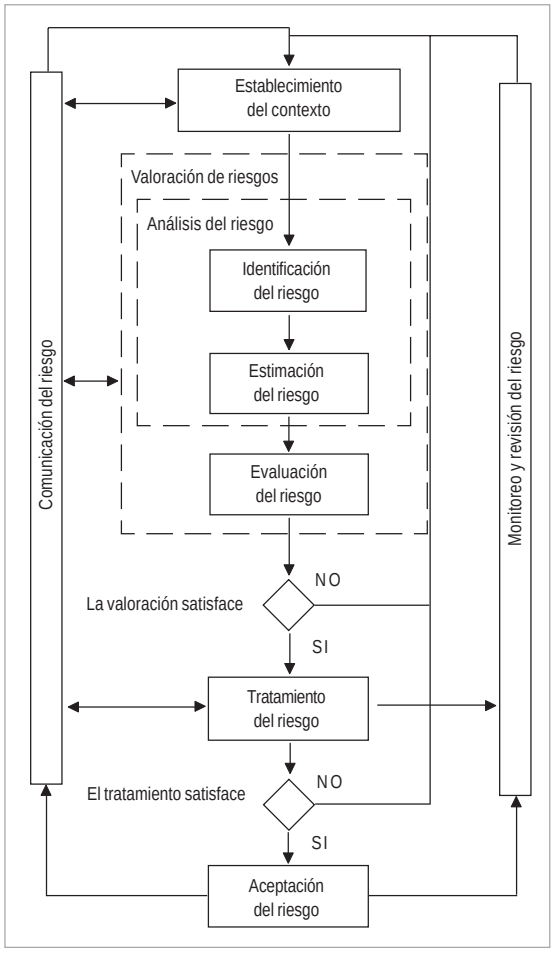

Figura 4. Proceso para gestión de riesgos de acuerdo a ISO 27005.

- NTC/IEC 27002: Con este estándar se establecen pautas y principios generales para la implementación, mantenimiento y mejora de la gestión de seguridad. Cuenta con un amplio listado de objetivos de control y controles para el SGSI [12].
- MAGERIT: Metodología española para la gestión y análisis de riesgos de los sistemas de la información que en sus tres libros "Método", "Catalogo de elementos" y "Guía de técnicas" sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos.
- NIST SP 800-30: Guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos. La guía provee apoyo en los procesos de valoración y mitigación dentro de la gestión de riesgos.
- NTC 5254: Norma técnica colombiana para la gestión de riesgos adoptada de la norma AS/NZ 4360:2004. Es una guía genérica que sirve como fuente de verificación de definiciones y proceso de documentación.
- ITIL® v3: La librería de infraestructura de tecnologías de la información es un estándar internacional *de facto* que describe buenas prácticas para gestionar servicios de TI. La presente metodología aplica los procesos concernientes a gestión de incidentes, gestión de problemas y gestión de acceso, y el proceso de mejora continua.

3. Pasos de la metodología

La metodología sigue los pasos del proceso de gestión de riesgos de acuerdo a ISO 27005, la cual contempla las siguientes etapas (Figura 4):

- Establecimiento de plan de comunicación interno y externo.
- Definición del contexto organizacional interno y externo.
- Valoración de riesgos tecnológicos.
- Tratamiento de riesgos tecnológicos.

- Monitoreo y mejora continua del proceso de gestión.

A continuación se explicará el propósito de cada etapa.

3.1. Establecimiento de un plan de comunicación interno y externo

El plan de comunicación se debe realizar a nivel interno (áreas de la organización, empleados, directivos, socios) y externo (clientes, proveedores, entes reguladores, todos los anteriores si así se requiere), teniendo en cuenta las definiciones sobre la existencia del riesgo, los objetivos de la gestión, el debido informe de los avances del proceso y todo aquello que se considere necesario. Los medios a usar para comunicar el proceso de gestión dependen de las necesidades y disponibilidad de la organización, sin embargo como medios se sugieren las circulares, capacitaciones, presentaciones, campañas de concientización que son de fácil desarrollo y permiten llegar a todo el público objetivo, de igual forma la consideración de otros medios depende de la organización.

Por otra parte, el plan de comunicación debe ser diseñado de forma tal que permita crear conciencia en seguridad y evidencie la existencia de riesgos tecnológicos; si está bien estructurado permitirá lograr los objetivos de la gestión de forma satisfactoria, obtener información de soporte al análisis y colaborar en la planificación del proceso de gestión de riesgos.

La propuesta presentada para estructurar el plan de comunicación contiene tres etapas:

1. Comunicación inicial: en esta se incluye conceptos generales sobre riesgos, sus implicaciones, las ventajas de la gestión, entre otros aspectos.
2. Comunicación sobre la marcha: Durante esta etapa se busca mostrar los avances del proceso de gestión de riesgos para obtener retroalimentación y conseguir el apoyo y participación de todos los involucrados en la organización.
3. Comunicación de resultados: Con esta etapa de la comunicación se busca compartir y difundir los resultados obtenidos teniendo en cuenta los debidos filtros de información de acuerdo al público objetivo.

Las anteriores etapas de comunicación aplican igual a nivel interno o externo dependiendo de las determinaciones de la organización.

3.2. Definición del contexto organizacional interno y externo

Las organizaciones tiene un contexto interno que incluye misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normatividad entre otros. De igual forma interactúa con su medio por lo cual podemos indicar que tiene un contexto externo en el cual deben considerarse aspectos como la competencia, regulaciones legales que apliquen, economía, política, tecnología, cultura y los demás aspectos que se consideren necesarios. La importancia de entender estos aspectos es saber que requiere ser protegido y cuáles son las limitaciones existentes para esta protección.

Como fuentes de información se recomienda emplear documentación existente en la organización relacionada con calidad, seguridad, planeación estratégica y continuidad que brinden información que permitan posicionar a la organización con respecto a su

medio, entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones y las demás que se consideren necesarias.

El objetivo de esta etapa es conocer a la organización para determinar que los puede afectar a nivel interno y externo, que requieren proteger y de acuerdo a los recursos actuales como podría darse esa protección para establecer el nivel de aceptación de riesgo al cual están dispuestos, determinar los alcances y limitaciones existentes.

3.3. Valoración de riesgos tecnológicos

En la etapa de valoración de riesgos se identifican los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales se encuentran expuestos. En este punto se recomiendan posibles controles para mitigación de los riesgos.

Para la valoración se deben tener en cuenta los posibles activos que sean relevantes, incluyendo procesos, información, datos y activos de soporte. La valoración para activos de soporte debe incluir costos por adquisición, renovación o reposición, mantenimiento y tener en cuenta los factores de depreciación. Luego de establecer el listado de activos es posible validar si el alcance definido de forma preliminar es correcto o debe ser ajustado para cumplir con los propósitos.

También se deben tener en cuenta los tipos de amenazas que pueden presentarse (estas pueden ser físicas, lógicas o estratégicas y su origen puede ser natural, técnico, humano accidental o intencional), los daños que pueden implicar las amenazas, la determinación sobre las pérdidas causadas por los riesgos en términos de impacto (para esto se puede usar un análisis de impacto sobre el negocio, mejor conocido como BIA- *Business Impact Analysis*). A partir de lo anterior es posible determinar los controles y priorizar los riesgos.

Los controles a usar se clasifican en controles preventivos, controles detectivos, y controles correctivos. De igual forma dependiendo de si se usa o no una base tecnológica para la implementación, los controles pueden ser técnicos o no técnicos.

Como parte de la identificación es importante tener en cuenta las dependencias entre activos y procesos, la cadena de valor y el valor mismo por activo y proceso. Los procesos deben ser priorizados con el fin de determinar niveles de criticidad de los mismos. Las vulnerabilidades pueden ser determinadas por varios medios como la realización de pruebas y listas de chequeo. Las amenazas deben clasificarse de forma acorde y el análisis de su impacto con respecto a la frecuencia de ocurrencia es importante para la determinación correcta de los riesgos. En la valoración se pueden usar técnicas cuantitativas y/o cualitativas para la estimación de riesgos y hay formas variadas de presentación de la información como los vectores de ataque o las matrices, todo depende de los requerimientos, conocimientos, recursos y habilidades del personal de la organización.

3.4. Tratamiento de riesgos tecnológicos

Con la etapa de tratamiento de riesgos se establece e implementan las acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización, dentro de las acciones a tomar encontramos principalmente: reducir, aceptar, eliminar y transferir.

Como parte del tratamiento se definen las posibles acciones a seguir sobre los riesgos y se establece un plan de tratamiento según la priorización previa que se realizó. Este plan debe definir recursos, responsabilidades y actividades teniendo en cuenta las posibles restricciones a nivel económico, legal, temporal, técnico, operativo, político, cultural y las demás que sean determinadas. Los controles que sean recomendados deben incluir un análisis costo-beneficio (incluyendo costos de implementación y mantenimiento).

El plan debe ser documentado y finalmente definidas las políticas a seguir. Con la definición de políticas se establece los lineamientos base y se logra ejercer la línea de mando el don de mando requerida para cumplir con las definiciones de seguridad indicadas con anterioridad.

En este punto es importante que el plan sea consistente con las metas y objetivos en la parte de planificación del proceso de gestión, maneje tiempos acordes con los definidos al inicio y con el tiempo de vida útil de los activos, además de dar paso a la siguiente etapa de mejora continua. El plan de tratamiento debe definir los pasos pormenorizados para gestionar los riesgos sin dejar espacio a nuevos posibles riesgos que ocurran como consecuencia de errores en la implementación de las acciones del tratamiento mismo.

3.5. Monitoreo y mejora continua del proceso de gestión

Para esta fase el elemento primordial es el control de cambios, por lo cual el monitoreo debe realizarse sobre activos, procesos, vulnerabilidades, amenazas, controles, documentación de políticas y procedimientos con el fin de establecer acciones a seguir ante cambios (tales como agregar activos, riesgos o amenazas nuevas o que algo se modifique o requiera ser eliminado) y lograr que la gestión este continuamente actualizada para lograr evaluar indicadores de cumplimiento de los planes.

Con el monitoreo y la mejora continua se busca asegurar la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos de mitigación definidos. También, permite agregar al análisis riesgos nuevos que puedan aparecer luego de la definición de los planes teniendo en cuenta posibles cambios internos y externos.

A manera de resumen, la Figura 5 presenta los pasos definidos en la metodología propuesta.

4. Gestión de riesgo y continuidad de negocios

Parte fundamental de la continuidad de negocios es la gestión de incidentes y a su vez está se relaciona con la gestión de riesgos. La adecuada gestión de incidentes evita que sean activados los planes de continuidad de negocios, por ello es importante que las respuestas a incidentes sean efectivas y se tengan claros los riesgos que pueden estar asociados.

La materialización de riesgos puede implicar impactos grandes sobre el negocio, asociado a altos costos por recuperación e indisponibilidad de los servicios o productos que ofrece la organización. Cuando se realiza la valoración de riesgos dentro de la gestión de continuidad se tiene en cuenta la valoración del riesgo tecnológico y su efecto sobre los activos de información. Gracias a este análisis previo es posible realizar la identificación

de los requerimientos mínimos para la continuidad de las operaciones basado en las posibles interrupciones y con ello diseñar las alternativas estratégicas de operación y proceso.

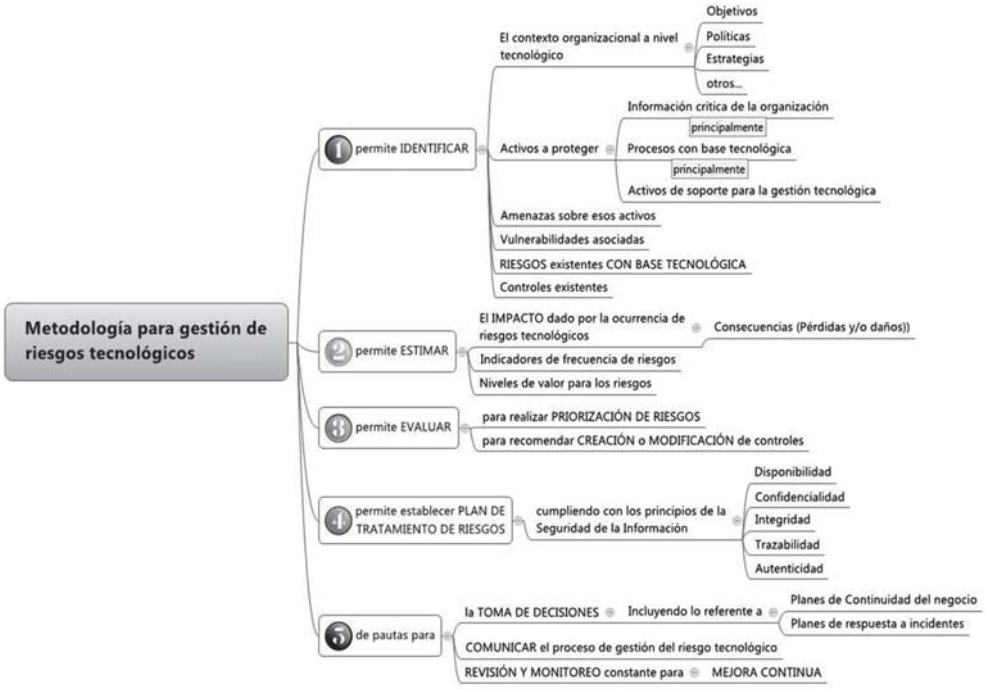

Figura 5. Pasos de la metodología para gestión

Como parte de las estrategias de continuidad se incluyen las acciones a tomar sobre los riesgos determinados, aceptándolos, evitándolos, transfiriéndolos o mitigándolos. De igual forma como parte de las opciones de mitigación se tienen en cuenta opciones de tipo tecnológico y no tecnológico.

Uno de los ejemplos más recordados y que mejor ilustra la necesidad de implementar planes de continuidad y gestión de riesgos fue el atentado del 11 de Septiembre al World Trade Center en New York, Estados Unidos. La tragedia implicó cambios en la concepción sobre la protección física y la seguridad informática que se requiere en las organizaciones [14]. Varias de las compañías que funcionaban en alguna de las torres gemelas se vieron fuertemente afectadas dado que no contaban con centros alternos de trabajo con capacidad de respuesta adecuada y planes de evacuación ante desastres.

A partir de esta nefasta fecha se enfatizó en la integración de sistemas *back-end* y la mejora de infraestructura. Organizaciones como la firma Merrill Lynch y Cantor Fitzgerald LP perdieron su centro de datos principal; la primera, cuya sede se encontraba cerca de la zona cero, estuvo inoperante por varias semanas; en el caso de la segunda, cuyo centro de operaciones se encontraba en una de las torres, tuvo una pérdida de vidas humanas cuantiosa, al igual que para el *holding* financiero y de componentes electrónicos que integraban a las marcas Cantor Fitzgerald, eSpeed y TradeSpark [15] [16].

A raíz de lo anterior, varias organizaciones desplazaron sus centros de datos a zonas de menor riesgo e iniciaron o reforzaron labores de teletrabajo a través de redes privadas virtuales, computación en la nube y planes a nivel de recuperación de operaciones cuidando de la integridad del personal.

Como se puede observar, aún hoy en día se encuentran carencias en la gestión de riesgo de algunas organizaciones, inclusive de gran tamaño. A nivel de empresas latinoamericanas recientemente la organización Coleman Parkes Research realizó una investigación donde encontraron que solo una tercera parte de estas organizaciones cuentan con una estrategia de gestión de riesgos, lo cual crea mayor exposición por la toma de medidas reactivas sobre las medidas de prevención. Las encuestas revelaron que el riesgo no se mide de forma directa y los procesos son manuales por lo cual el control no es adecuado. Los ejemplos anteriores, muestran que la gestión de riesgos debe ser vista como soporte a la gestión de continuidad de negocios y la recuperación ante desastres [17].

5. Conclusiones

La metodología propuesta presenta una oportunidad para entender mejor los conceptos definidos en los estándares mencionados para gestión de riesgos dándole un enfoque a los riesgos tecnológicos. Esta brinda un mapa de ruta para la aplicación del proceso de gestión de riesgos de 27005 evitando los vacíos y ambigüedades que tienen los estándares ISO, dando indicaciones sobre cómo llevar a cabo las acciones que estos mencionan. Como parte del desarrollo y evaluación de la metodología se realizó la evaluación y tratamiento de riesgos en una organización con un fuerte componente tecnológico encontrando la posibilidad de mitigar en un 70% los riesgos de origen tecnológico presentes (para una descripción detallada se puede consultar [1]).

La gestión de los riesgos tecnológicos es importante dado que las organizaciones al usar tecnología en su actividad diaria y como parte de sus procesos de negocio se encuentran expuestas a este tipo de riesgos; por ello pueden afectar la actividad propia de las mismas y ser fuentes de pérdidas y daños considerables. De lo anterior los planes de seguridad deben enfatizar en crear conciencia en seguridad para prevenir riesgos y buscar estrategias para obtener el apoyo de la alta dirección con el fin de cumplir con los objetivos y asegurar la información crítica, adicional la gestión adecuada de los riesgos permite evitar en gran medida la ocurrencia de incidentes y con ello evitar la activación de planes de continuidad. Las organizaciones deben robustecer su protección a nivel físico (lo correspondiente a infraestructura, incluyendo la tecnológica), nivel lógico (sistemas de información y software) y factor humano (toma de medidas organizacionales); en estos tres aspectos está presente el uso de tecnología y por ello la exposición a este tipo especifico de riesgo crece constantemente. Esta es la motivación de la metodología descrita, como punto de partida para dar lineamientos sobre cómo gestionar este tipo de riesgos integrando los tres aspectos mencionados y buscando un marco de protección integral.

Finalmente, es necesario resaltar que sin importar el ámbito en el que se encuentra una organización se requiere la aplicación de gestión de riesgos. Para muchas organizaciones la toma de medidas preventivas, que es el principal punto de la gestión de riesgos, y la continuidad de negocios puede pasar como irrelevante, pero en su debido cuidado radica la disminución de pérdidas y perjuicios.

Referencias bibliográficas

[1] Caída en la red de Bancolombia genera caos en los usuarios del sistema. (Febrero 2011). Recuperado de http://www.rcn.com.co/noticias/16-02-11/ca-da-de-la-red-en-bancolombia-gener-caos-en-los-usuarios-del-sistema.

[2] Ramírez Castro, Alexandra. (2012). Desarrollo de una metodología para la gestión del riesgo tecnológico a partir de ISO 31000 e ISO 27005. Tesis de grado para optar como Ingeniera de sistemas, Proyecto curricular de ingeniería de sistemas, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

[3] ISO (International Standard Organization). (2011). Gestión del riesgo – Principios directrices. Estándar de Seguridad ISO 31000.

[4] ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

[5] Ministerio de administraciones públicas. (2006). MAGERIT - Metodología de análisis y gestión de riesgos de los sistemas de información – Método, Versión 2, España.

[6] NIST (National Institute of Standards and Technology). (2002). NIST SP 800-30. Guía de Gestión de riesgo para sistemas de tecnología de la Información – Recomendaciones del Instituto Nacional de Estándares y Tecnología.

[7] ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación). (2006). Gestión de riesgo, NTC 5254 - Norma Técnica Colombiana.

[8] ISO (International Standard Organization). (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Estándar de Seguridad ISO/IEC 27001,.

[9] OGC (Office of government commerce). (2009). ITIL® V3 Foundation – Study guide book and online course. The art of service.

[10] The Business Continuity Institute. (2010). Guía de buenas prácticas. Una guía de gestión para la implementación de buenas prácticas en la gestión de la continuidad del negocio.

[11] Orientación acerca del enfoque basado en procesos para los sistemas de gestión de la calidad. (Mayo 2001). Recuperado de http://www.iram.com.ar/Documentos/Certificacion/Sistemas/ISO9000_2000/procesos.pdf.

[12] ISO (International Standard Organization). (2005). Tecnología de la Información – Técnicas de seguridad – Código de prácticas para la gestión del a seguridad de la información. Estándar de Seguridad ISO/IEC 27002.

[13] Kent Anderson. (2008). A business Model for information Security. Recuperado de http://www.isaca.org/Journal/Past-Issues/2008/Volume-3/Documents/jpdf0803-a-business-model.pdf

[14] Thibodeau, Patrick. Computerworld. (Septiembre 2011). Computerworld: Como cambio el 11 de septiembre a los centros de datos. México. Recuperado de http://www.computerworldmexico.mx/articulos/18239.htm?goback=.gde_128300_member_162326734

[15] Computerworld. (Septiembre 2011). Computerworld: Lecciones aprendidas para la recuperación de desastres tras el 9/11. México. Recuperado de http://www.computerworldmexico.mx/Articulos/18319.htm

[16] Strozza, Pedro. (2001). Clarin.com: Las empresas que funcionaban en las Torres Gemelas intentan volver a la normalidad. Argentina. Recuperado de http://edant.clarin.com/diario/2001/10/12/i-309412.htm

[17] Ruiz Vega, Carolina. (Septiembre 2012). Cryptex – Seguridad de la información: Dos tercios de las empresas latinas carecen de una estrategia de gestión de riesgo. Recuperado de http://seguridad-informacion.blogspot.com/2012/09/dos-tercios-de-las-empreas latinas.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SeguridadDeLaInformacion+%28Seguridad+de+la+Informacion+link%3A+http%3A%2F%2Fseguridad informacion.blogspot.com%29

Alexandra Ramírez Castro

Ingeniera de Sistemas de la Universidad Distrital Francisco José de Caldas. Se encuentra estudiando la Maestría en Seguridad de las Tecnologías de la Información y las Comunicaciones. Certificada como auditor interno BS 25999 (Gestión de continuidad de negocios) e ITIL Foundations v3 (Gestión de servicios de tecnología). Tiene estudios complementarios en gestión de proyectos y seguridad de la información.Ha trabajado como consultora en gestión de riesgos y actualmente está vinculada con el Banco de Bogotá.

Zulima Ortiz Bayona

Matemática de la Universidad Nacional de Colombia, Msc en Matemáticas de la Universidad Nacional de Colombia, Especialista en Teleinformática de la Universidad Distrital Francisco José de Caldas. Actualmente se desempeña como profesora de tiempo completo de la Facultad de Ingeniería de la Universidad Francisco José de Caldas. Sus áreas de interés son la criptografía y la seguridad informática.