Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA

Neftali Esaú López Marcos
Asesorado por el Ing. Juan Carlos Morales Baten

Guatemala, octubre de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

NEFTALI ESAÚ LÓPEZ MARCOS
ASESORADO POR EL ING. JUAN CARLOS MORALES BATEN

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

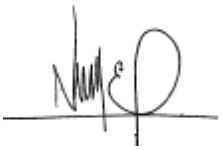
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. Juan Álvaro Díaz Ardavin
EXAMINADOR	Ing. Cesar Rolando Batz Saquimux
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha marzo de 2011.



Neftali Esaú López Marcos

Guatemala, 27 de junio de 2011

Ing. Carlos Azurdia Morales
Coordinador de Revisión de Trabajo de Graduación
Carrera de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Respetable Ingeniero Azurdia

Por este medio le informo que como asesor del trabajo de graduación del estudiante universitario de la carrera de Ingeniería en Ciencias y Sistemas, Neftali Esaú López Marcos, carné 93 12535, he revisado y a mi criterio el mismo cumple los objetivos propuestos para su desarrollo, según el protocolo del trabajo de graduación titulado: "GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA".

Sin otro particular me suscribo de usted,

Atentamente,

Ing. Juan Carlos Morales
Colegiado No. 2623

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 13 de Julio de 2011

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **NEFTALI ESAÚ LÓPEZ MARCOS** carné **1993-12535,** titulado: **"GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA",*** *presentado por el estudiante NEFTALI ESAÚ LÓPEZ MARCOS, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Turk
Director, Escuela de Ingeniería Ciencias y Sistemas

Guatemala, 17 de octubre 2011

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 414.2011

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **GESTIÓN DE RIESGOS CORPORATIVOS DE TI EN GUATEMALA,** presentado por el estudiante universitario **Neftali Esaú López Marcos,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, 18 de octubre de 2011.

/gdech

ACTO QUE DEDICO A:

El Shaddai	En honor al Señor Dios Todopoderoso, gracias Padre por todo lo que me has dado. Gracias por tu Espíritu Santo y tu Hijo Jesucristo Rey de Reyes y Señor de Señores.
Mis padres	Cándido López Ramírez y Dina Marcos de López, por su amor, consejo, su ejemplo y la ayuda que he recibido en toda mi vida.
Mi esposa	Lesbia, por su amor incondicional, por complementar mi vida de una forma muy especial.
Mi hijo e hijas	Cristian, Gabriela y Andrea, por su amor y alegrarme la vida.
Mis hermanos y hermanas	Lidia, Luis, Emma, Dora y Mynor, porque siempre he obtenido su amor y apoyo incondicional.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

COSO El Comité de las Organizaciones Patrocinadoras de la Comisión Treadway (COSO, proviene de “Committee of Sponsoring Organizations of the Treadway Commission”) definió un marco de trabajo que describe los componentes necesarios para la gestión de riesgos empresariales.

ERM Acrónimo de Enterprise Risk Management (Gestión de riesgos empresariales o corporativos).

ERP Los sistemas de planificación de recursos empresariales (ERP, proviene de ”Enterprise Resource Planning”) son sistemas de información que permiten administrar e integrar diferentes recursos y procesos en las empresas.

GRC Acrónimo que se refiere a gobierno, riesgo y cumplimiento.

IEEE El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, proviene de “Institute of Electrical and Electronics Engineers”) es una asociación profesional dedicada a la estandarización.

ISACA	Acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control para Sistemas de Información) cuya visión es ser el líder en gobierno de TI, control y aseguramiento.
Outsourcing	Outsourcing (subcontratación), es la contratación de servicios o recursos a otra empresa, usualmente por medio de un contrato legal que regula la relación.
PMBOK	PMBOK (siglas de “Project Management Body of Knowledge”) es un estándar en la administración de proyectos desarrollado por PMI.
PMI	El instituto de administración de proyectos (PMI, proviene de “Project Management Institute”) es una organización internacional que reúne profesionales relacionados con la gestión de proyectos.
TI	Acrónimo que se refiere a las Tecnologías de la Información.

RESUMEN

En el medio corporativo empresarial en Guatemala, las empresas desean ser cada vez más competitivas y buscan obtener el mejor beneficio con los recursos que disponen utilizando para ello la tecnología.

Debido a ello, los ingenieros en sistemas y el personal responsable de las tecnologías de la información en las organizaciones, deben tener conciencia sobre la existencia de los riesgos relacionados, y administrarlos adecuadamente. La gestión de riesgos de TI requiere del conocimiento de los principios y conceptos que la sustentan y de comprender las acciones que se deben realizar para que los objetivos organizacionales sean alcanzados.

Los riesgos son explicados haciendo uso de escenarios genéricos que abarcan diferentes áreas de TI. Inmersos en el ámbito guatemalteco, se presentan también escenarios con enfoque en el cumplimiento legal de TI.

En Guatemala, el medio corporativo presenta resultados aceptables respecto de las acciones que se han realizado para reducir las consecuencias de los riesgos. Las respuestas obtenidas en una encuesta realizada al personal de IT lo confirman.

Para administrar los riesgos se plantea un marco de trabajo que consiste en un proceso de mejora continua, orientado a las actividades necesarias para obtener los resultados esperados de TI en la organización. Como elemento fundamental, se indican los controles requeridos para responder a los riesgos en los diferentes escenarios.

OBJETIVOS

General

Apoyar a los ingenieros que asumen responsabilidades de dirección en la gerencia de tecnologías de información y a los responsables de la gestión de riesgos del área de informática, por medio de un marco de trabajo, aplicable en el entorno guatemalteco.

Específicos

1. Presentar los conceptos relacionados con la gestión de riesgos corporativos de TI.

2. Comprender los riesgos potenciales a nivel corporativo, relacionados con TI.

3. Obtener información a nivel corporativo sobre cómo las empresas en el medio guatemalteco gestionan los riesgos.

4. Plantear un marco de trabajo que permita una adecuada gestión de los riesgos que se enfrentan en TI en el entorno guatemalteco.

INTRODUCCIÓN

El crecimiento del uso de tecnologías de la información en el medio corporativo guatemalteco requiere que los profesionales se mantengan actualizados, para optar a mayores beneficios en el desempeño de sus actividades con los recursos de que disponen.

Las empresas observan cómo el uso de las tecnologías modernas permite nuevas oportunidades para realizar los negocios de diferentes maneras, hacer productos con mayor calidad y dar a sus clientes servicios innovadores, entre otras ventajas.

Sin embargo toda oportunidad conlleva riesgos de diferente índole y dependiendo de las circunstancias en las que ocurran, puede afectar de una o de otra forma los resultados que se desea obtener.

Este estudio presenta una base conceptual con orientación práctica acerca de los riesgos relacionados con el uso de las tecnologías de la información. Además, en él se abordarán los riesgos desde una perspectiva ejecutiva y también desde el punto de vista del personal que labora dentro del área de informática, durante la realización de sus actividades diarias.

Adicionalmente, se presentará un marco de trabajo para la gestión de riesgos que sirva de guía a los ingenieros que asumen responsabilidades de dirección en la gerencia de tecnologías de información y también para aquellos que sean responsables de la gestión de riesgos del área de informática.

1. MARCO TEÓRICO

1.1. Riesgos

En toda actividad que se realice en cualquier ámbito existen riesgos. Un riesgo, según la enciclopedia libre Wikipedia, es la posibilidad de que una persona, empresa, entidad o cosa perciba un daño o perjuicio y como resultado afecte su valor óptimo esperado.

Los riesgos surgen por la existencia de eventos voluntarios o involuntarios que tienen probabilidades de ocurrir y que al materializarse pueden ocasionar daños, perjuicios o afectar la obtención del valor esperado. Si se utiliza un ejemplo de la vida cotidiana como el trasladarse de un lugar a otro utilizando un vehículo en la ciudad de Guatemala, desde un punto A hacia un punto B en un período de tiempo, podrá observarse que existe la probabilidad de que algunos eventos no deseados se presenten e impidan que la actividad se lleve a cabo.

Por ejemplo, puede ocurrir una fuerte lluvia e inundar algunas de las calles sobre las cuales se tenía considerado transitar. Para ser proactivo sobre la existencia de este evento, se recomienda tomarse unos minutos previos para investigar el clima en la ciudad y en caso de que exista un pronóstico de lluvias, se debe evaluar la posibilidad de tomar rutas alternas con menor flujo de vehículos y utilizar un horario que no sea hora pico en la ciudad de Guatemala.

La existencia misma de los riesgos motiva a prepararse con anticipación para poder evitarlos, para saber qué se debe hacer con ellos en caso se presenten. Las actividades que se realizan durante el uso de las tecnologías de Información TI también tienen diferentes riesgos y se debe tener la capacidad de gestionarlos apropiadamente para evitar sus efectos y generar el valor esperado.

1.2. Riesgos corporativos de TI

Desde una perspectiva integral, una organización empresarial puede ser afectada por diferentes riesgos entre los que deben ser incluidos los riesgos corporativos relacionados con el uso de las tecnologías.

En el contexto de TI existen muchas áreas donde pueden ocurrir riesgos. Riesgos relacionados con la disponibilidad y recuperación de los sistemas, con la generación de valor al negocio de acuerdo con las estrategias gerenciales, la administración del cambio de las aplicaciones, la gestión de problemas, el cumplimiento de acuerdos de servicio con los clientes de TI, la gestión de proyectos, la gestión de proveedores, la seguridad de la información, la seguridad de los bienes físicos de TI, el personal, la integridad de la información, la seguridad de las redes para acceso interno y externo, el uso de dispositivos móviles, el respaldo y recuperación de datos y otros más.

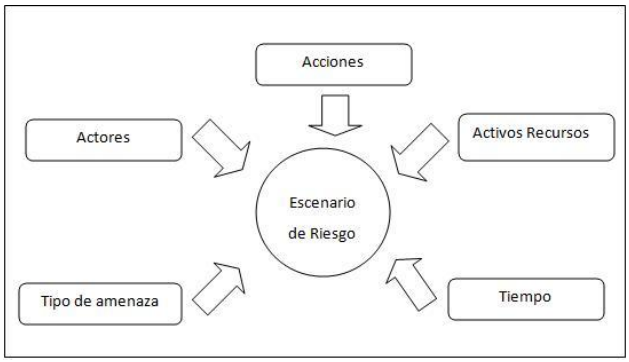
Otros riesgos existentes en las organizaciones tienen que ver con la estrategia del negocio, el cumplimiento interno y externo, los procesos operacionales internos, los procesos de entrega de productos y servicios propios de la naturaleza de la organización, y el ambiente externo.

En consecuencia, son muchos los eventos que se pueden presentar en cualquiera de las partes que componen TI y desencadenar problemas que pueden impactar negativamente en la organización y causar daños o pérdidas en diferente grado de severidad. Es por ello que se hace necesario administrarlos adecuadamente cuando se presenten, hasta reducirlos a un nivel aceptable para el negocio.

1.2.1. Escenarios de riesgos

Según el marco de trabajo de riesgos de IT, de ISACA, a la explicación de un evento que representa un riesgo en un ambiente de TI, se le llama escenario del riesgo. Los elementos que forman el escenario de riesgo se presentan en la siguiente figura:

Figura 1. **Componentes del escenario del riesgo**



Fuente: ISACA http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-framework-spanish.pdf

Para que un riesgo se materialice o se pueda simular en el tiempo con el propósito de analizarlo, es necesario que algunos elementos entren en acción. Los elementos que forman parte del escenario del riesgo son: actores, tipo de amenaza, acciones, activos o recursos y el tiempo.

El actor es quien está involucrado directamente en el evento, pueden o no ser personas y también pueden formar parte de la organización.

Otro componente es el tipo de amenaza, el cual constituye una forma de clasificar el evento. Puede ser causado por una acción malintencionada, algún efecto de la naturaleza, un accidente, o simplemente el resultado de realizar alguna operación común, de forma no estándar, fuera del procedimiento establecido.

La acción que se realiza se identifica fácilmente porque es un hecho o una actividad. Ejemplos de acciones son el uso indebido, omisión de una norma, interrupción, modificación, robo y otras. Toda acción tiene efecto sobre un activo, bien o recurso de la organización, el cual constituye un elemento de valor dentro de la empresa. Todos los activos pueden clasificarse de acuerdo con un nivel de importancia y es necesario enfocarse con mayor interés en aquellos que son críticos. Ejemplos de recursos son: la infraestructura de TI y las aplicaciones (conocidas también como software).

El último componente de un escenario del riesgo es el tiempo. Se refiere a que a veces el tiempo es un elemento muy importante y a veces no lo es, eso dependerá del evento en sí y de factores como duración del mismo. Por ejemplo: el instante del día o fecha en el que ocurre, la cantidad de tiempo entre el evento y el tiempo en que los efectos de daño o perjuicio se materialicen.

1.2.2. Factores de riesgos

En el marco de trabajo de riesgos de TI, de ISACA, los factores de riesgos dentro de un contexto de escenarios de riesgo, son los elementos que contribuyen con la frecuencia e impacto sobre los activos o recursos de una organización.

Los factores de riesgos pueden representar situaciones o debilidades que facilitan el hecho que los escenarios de riesgo cobren vida. Estos pueden estar dentro del control de la organización; sin embargo existen factores que son ajenos o externos y no se tiene influencia sobre ellos y por tanto no pueden suprimirse, aunque si se gestionan apropiadamente, pueden minimizar el daño o perjuicio ocasionado por los mismos.

Un ejemplo de factor de riesgo, es la capacidad de una organización para gestionarlos. Existirán empresas que no gestionen los riesgos de TI de ninguna manera, o que solo lo hagan superficialmente. Este factor impactará con mayor fuerza en la medida en que la organización no esté preparada. Y en los casos en que la empresa tenga un nivel alto de madurez en su gestión de riesgos, el impacto será menor.

Otro ejemplo, es la falta de lineamientos o políticas para una o más actividades operativas relacionadas con TI, lo cual puede impactar en la organización, en que la realización de tales actividades se haga de forma inadecuada o incorrecta.

Los factores de riesgos, según la guía profesional de riesgos de TI, de ISACA, pueden ser clasificados como internos o externos a la organización.

Entre los factores del ambiente interno en la organización se tiene:

- La importancia estratégica de TI. Por ejemplo, si es utilizada para cubrir las operaciones básicas de la organización o en la generación de nuevos productos y servicios que incrementen el valor de la organización.

- La complejidad del negocio. Es relevante porque a pesar de ella, los servicios y recursos de TI deben ser puestos a disposición de la empresa. La complejidad puede ser vista en perspectiva física y operativa. Los factores físicos existen debido a que la empresa puede tener una estructura interna amplia con muchas secciones o ubicaciones, por ejemplo muchas agencias de un banco, varios puntos de venta para un supermercado, una o más plantas de producción y varios puntos de distribución. La otra perspectiva es la operativa, considerando diversas actividades, servicios o productos relacionados con el giro del negocio.

- Capacidad de cambio del negocio. Qué tan flexible es la organización al cambio. Por ejemplo: ¿Qué tan fácil o difícil es para la organización asimilar nuevos productos, desde su fabricación, distribución y venta? ¿Qué tan fácil o difícil es para la organización implementar un cambio de sistema?

- Cultura organizacional. ¿Cómo es la cultura interna respecto de los principios y valores? Una empresa que los ha fomentado y los lleva a la práctica se hace diferenciar de otras. No obstante, aquellas que carecen de ellos, se exponen a la ocurrencia de riesgos por incumplimientos internos o legales. Por ejemplo el uso y adquisición de software sin licenciamiento.

- Capacidad interna de TI. ¿Cómo está estructurada y organizada para proveer los recursos y servicios? ¿Cuáles son las metodologías, estándares o marcos de trabajo que se utilizan para realizar las actividades? El negocio puede llegar a tener mucha dependencia de TI para la realización de sus operaciones y por ello es imprescindible tener orden y utilizar las prácticas que influyan positivamente a favor de la organización.

- Capacidad para administrar TI. Según sea la estrategia definida para TI, cabe resaltar que las acciones de la alta dirección respecto de cómo, cuándo y cuánto se debe invertir, son trascendentales para garantizar el mayor rendimiento y aprovechamiento de los recursos de TI.

- Capacidad para administrar los riesgos en la organización. El nivel de madurez que se tenga para la gestión de los riesgos corporativos es un factor importante, porque de ello depende el impacto y frecuencia de los mismos en la organización.

Entre los factores de riesgos del ambiente externo a la organización se tiene:

- El entorno regulatorio y legal del país. Por ejemplo cambio en las leyes del país, nuevos lineamientos de entidades como la Superintendencia de Bancos que regula el sector financiero del país.

- La situación geográfica y política que tiene Guatemala. Por ejemplo la probabilidad de existencia de sismos, el efecto del invierno en la infraestructura del país, el estatus del ambiente de seguridad.

- El entorno tecnológico que cambia constantemente.

- La competencia. Puede influir en la disminución de los clientes o disminución de ventas por nuevos productos o servicios. Otro ejemplo: pueden contratar a una o más personas claves del equipo de TI.

- La situación económica. Por ejemplo la inflación y la tasa de cambio que influyen en los costos cuando se trata de adquisición de nuevos equipos o servicios.

1.2.3. Riesgos organizacionales

Según el estudio de concepto de riesgo publicado en el sitio Web Slideshare, los riesgos organizacionales son todos aquellos que de llegar a materializarse, generarán una variación en los resultados esperados. Esto significa que pueden causar daños personales, daños a bienes o servicios, o disminuir el rendimiento esperado, disminuir la calidad de un producto fabricado, incrementar los costos relacionados con un trabajo realizado, incrementar el tiempo de realización de una actividad que representa incumplimientos a compromisos preestablecidos y muchos más.

Una forma de organizar los riesgos es la que utiliza el modelo para control interno de las empresas COSO ERM, el cual se enfoca en los objetivos empresariales clasificándolos en cuatro categorías: estrategia, operación, información y cumplimiento.

De acuerdo con el resumen ejecutivo de COSO, respecto a la clasificación de los objetivos empresariales, la gestión de los riesgos organizacionales puede realizarse de arriba hacia abajo, es decir desde el nivel estratégico hasta llegar hacia los niveles operativos más detallados.

1.2.4. Riesgos relacionados con TI

Los riesgos de TI pueden encontrarse en todas las actividades operativas y estratégicas lo cual es comprensible y previsible debido a que efectivamente las tecnologías de la información influyen en las operaciones de cualquier empresa, con el objetivo de generar valor.

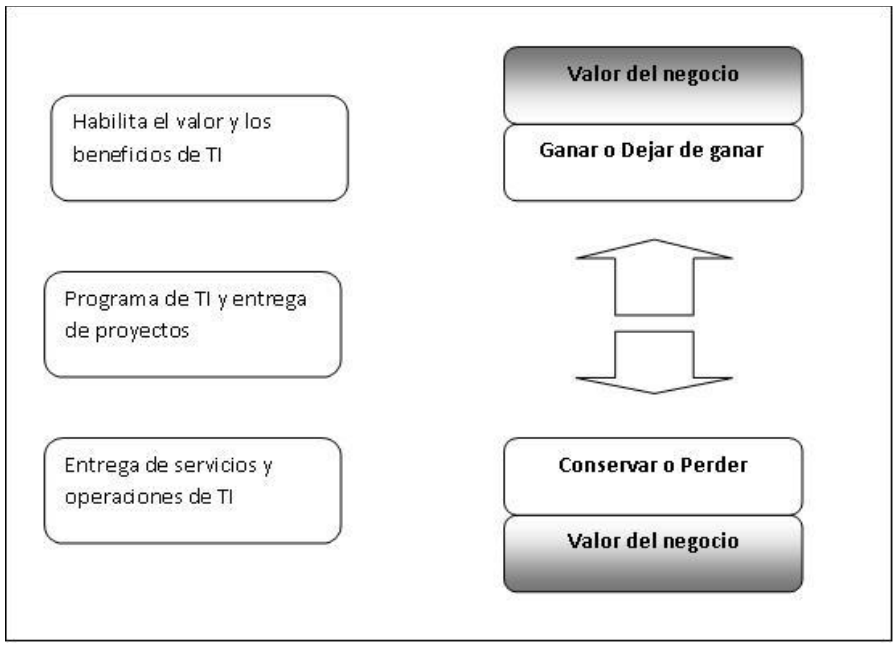
Se conoce que los riesgos materializados por el uso de la TI pueden provocar daño o perjuicio a bienes o activos en una organización, también que su uso permite generar valor al negocio, optimizar el uso de los recursos empresariales, apoyar la efectividad de sus procesos internos, diferenciar a la empresa de su competencia y favorecer nuevas oportunidades de negocio. Existe una relación entre la gestión de riesgos y el beneficio que se puede recibir.

Los riesgos relacionados con TI pueden clasificarse de diferentes maneras, por ejemplo, organizarlos de acuerdo con la estructura interna del área de TI donde pueden ocurrir, esto es infraestructura, aplicaciones y servicios. Otra forma de clasificarlos es de acuerdo con los objetivos de TI.

Según el marco de trabajo de riesgos de TI, de ISACA, existe la perspectiva basada en que la gestión de riesgos sirve como una herramienta de negocio que motiva la generación de valor y protege a la organización de pérdidas o daños.

La figura 2, que está a continuación, muestra la clasificación de riesgos desde una perspectiva de valor para la organización.

Figura 2. **Categorías de los riesgos de TI y el valor ganado o perdido**



Fuente:http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-framework-spanish.pdf

Se muestra cómo al utilizar la TI se pueden presentar riesgos que hacen perder valor al negocio y que se traduce en daños de diferente índole. No obstante al gestionar adecuadamente los riesgos, el valor para la organización puede mantenerse e incrementarse. En los riesgos se presentan la posibilidad de que el valor sea ganado o perdido.

Los eventos y factores existentes en los escenarios de riesgo unidos a las acciones de respuesta que se ejecuten, llevarán los resultados hacia la obtención de los beneficios o hacia asumir las pérdidas.

1.2.5. Portafolio o perfil de riesgos

En la perspectiva empresarial, según el documento acerca de ERM publicado en el sitio Web de la Universidad de la República, en Uruguay, un portafolio de riesgos llamado también perfil de riesgos, constituye la visión contextual y total de los riesgos. Constituye un inventario descriptivo y completo de riesgos de TI conocidos, contiene información sobre los procesos de negocio y los riesgos a los cuales la organización está expuesta.

1.3. Gobierno del riesgo

El gobierno del riesgo es un concepto utilizado dentro del marco de trabajo Risk IT, de ISACA. El objetivo del gobierno de riesgo consiste en asegurar la gestión de riesgos de TI en toda la organización y debe establecer un marco de administración de riesgos de TI.

Significa que se debe realizar actividades que permitan evaluar cada uno de los riesgos relacionados, sugerir y plantear los límites de tolerancia, según sea beneficioso para la organización.

1.3.1. Apetito del riesgo

El apetito del riesgo, de acuerdo con el marco de trabajo de riesgos de TI, de ISACA, es el valor de riesgo máximo que la empresa está dispuesta a aceptar, teniendo en consideración que se desean alcanzar los objetivos del negocio que han sido establecidos. Se puede expresar en términos de magnitud y frecuencia. Para explicar de forma gráfica el apetito del riesgo se permite utilizar mapas de riesgos, que se describen más adelante.

1.3.2. Tolerancia

La tolerancia del riesgo: se llama así a la variación aceptable en el logro de los objetivos, según lo describe el marco de trabajo de riesgos de TI, de ISACA.

1.3.3. Riesgo inherente

Según el marco de trabajo de riesgos de TI, de ISACA, se refiere al riesgo que por su propia naturaleza tiene asociado cada proceso. Representa el riesgo sin considerar ninguna de las acciones que se puedan realizar para gestionarlo.

1.3.4. Riesgo residual

De acuerdo con el marco de trabajo de riesgos de TI, de ISACA, representa el riesgo que queda después de haber realizado las acciones definidas para responder al mismo.

En la gestión de riesgos, se busca que el riesgo residual alcance un nivel aceptable para el negocio.

1.3.5. Indicadores de riesgos

Los indicadores del riesgo se utilizan como un instrumento de medición que permite evaluar si un riesgo tiene probabilidad de ocurrir y también ayudan a identificar si los valores esperados están acordes a los niveles aprobados.

Los indicadores de riesgos permiten diagnosticar el estado de los riesgos en el transcurso de las actividades que se realizan en el entorno de TI y con ello obtener una alerta a su debido tiempo, para que se pueda evitar o mitigar la materialización de un riesgo.

Cabe mencionar que todas las empresas poseen características internas que las hacen diferentes; es por ello que al implementar el uso de indicadores de riesgo se debe evaluar cuáles son factibles dentro de la organización.

Los factores que pueden ayudar a seleccionarlos son: el impacto del riesgo, el esfuerzo que requiere el utilizarlo, lo fiable de sus resultados y la capacidad de ser sensibles a la variación de tolerancia que el negocio acepte.

1.3.6. Cultura de riesgos

La cultura de riesgos implica que dentro de la organización exista una conciencia hacia los riesgos y cómo gestionarlos; esto significa que se comprende el porqué se deben tratar y cómo debe hacerse.

Hay tres elementos que se deben considerar al hablar de cultura de riesgos:

- ¿Cómo se conduce la organización al encarar un riesgo? Una organización puede actuar de forma conservadora o agresiva o tomar una actitud intermedia.

- ¿Qué ocurre cuando los resultados son adversos o negativos? Un resultado adverso puede implicar percibir un daño o pérdida de una oportunidad. La cultura de riesgos determinará si se maneja un enfoque de culpa o de aprendizaje y adaptación.

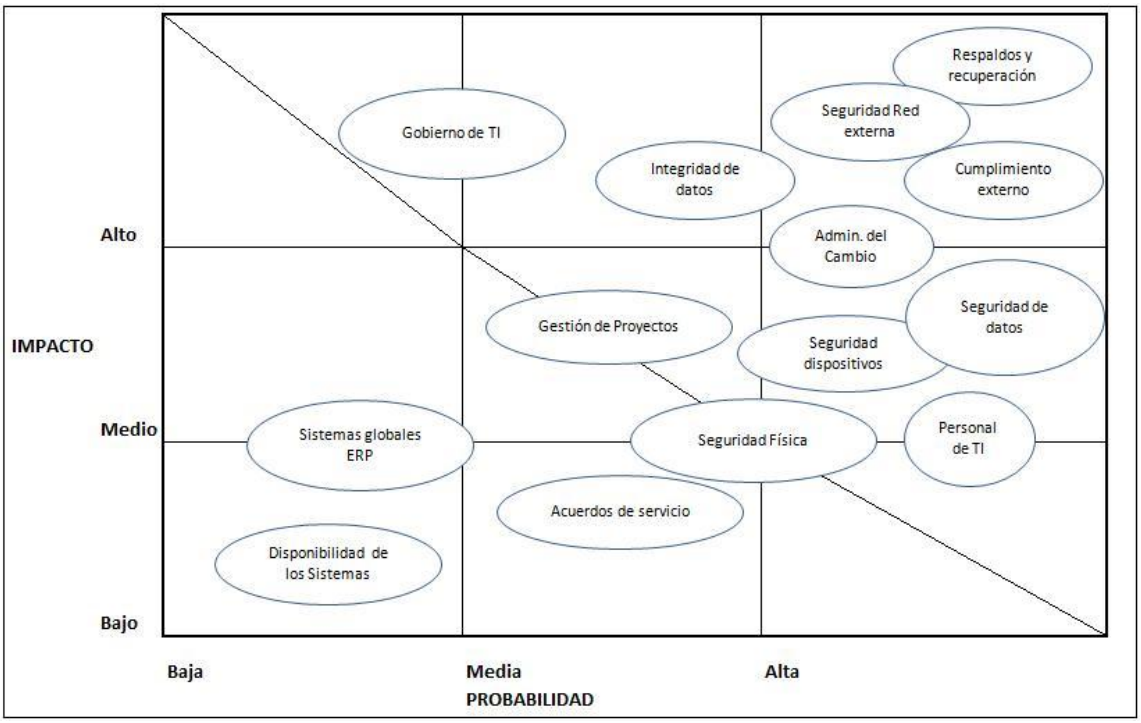
- ¿Se aceptan, rechazan o cumplen las políticas implementadas? Es importante que las políticas se comuniquen oportunamente y con claridad, exponiendo los beneficios y daños que conlleva su cumplimiento o incumplimiento, respectivamente.

1.4. Mapas de riesgos

Un mapa de riesgos es un instrumento gráfico que presenta uno o más riesgos en el contexto de la frecuencia, impacto en el negocio y probabilidad de ocurrencia. Usualmente se consideran dos dimensiones, por ejemplo: probabilidad e impacto, o frecuencia e impacto.

En la siguiente figura se muestra un ejemplo de un mapa utilizando las dimensiones de probabilidad e impacto de riesgos. Se presentan algunos riesgos relacionados con TI y se ubican dentro de una escala de probabilidad con los posibles valores: baja, media y alta. La otra medición es en relación con el impacto en el negocio, con los posibles valores: baja, media y alta.

Figura 3. **Mapa de riesgos**



Fuente: Revista ISACA Journal Risk Management and Assessment. Volumen 1 2010

1.5. Principios acerca de los riesgos

Para relacionar los riesgos en un ambiente empresarial es útil definir un conjunto de principios que expresan el vínculo entre la organización y los riesgos. Según el modelo GRC y el marco de trabajo de riesgos de TI, de ISACA, los principios se describen a continuación:

- Los riesgos se definen en términos de protección y generación de valor para la organización.

- La gestión de riesgos de TI se evalúa y alinea constantemente con los objetivos de la organización.

- Los recursos empresariales de gestión de riesgo corporativo son utilizados para la gestión de riesgos de TI, debido a que forman parte de ellos.

- Un marco de riesgos debe ser utilizado para su correcta administración.

- Debe existir una definición clara de los roles, los responsables y la especificación de las personas con autoridad dentro de la organización.

- Las entidades externas o internas de control, privadas o del Estado, deben tener visibilidad sobre las prácticas de gestión de riesgos implementadas y sus resultados.

- La comunicación debe ser eficaz.

- La gestión de riesgos motiva a una cultura de riesgos, que ha permeado la organización en su trabajo diario.

2. GESTIÓN DE RIESGOS TI

La gestión de riesgos consiste en dirigir todas las actividades necesarias para asistir a las organizaciones en busca de obtener mayores beneficios, reduciendo el efecto de los mismos, a un valor aceptado por el negocio cuando se utilizan recursos o servicios de TI.

Existen estándares y marcos de trabajo para tratar los riesgos empresariales y que pueden aplicarse en TI, por ejemplo: el estándar ISO 31000:2009, los marcos de trabajo COSO ERM del *Committee of Sponsoring Organizations of the Treadway Commision* (COSO) y el marco de trabajo Risk IT, de ISACA.

Al hablar de gestión de gestión de riesgos de TI se debe aclarar que esta actividad empresarial debe formar parte de la gestión de riesgos corporativos, aunque también se comparte la responsabilidad con los niveles gerenciales de TI.

Es importante tener un punto de inicio y evaluar el estado actual de su administración dentro de la organización para poder determinar las actividades que deben ser ejecutadas y los recursos necesarios. Para conocer el estatus actual de la empresa es necesario utilizar un modelo de referencia, el cual se describe a continuación.

2.1. Modelo de madurez para la gestión de riesgos de TI

De acuerdo con el marco de trabajo de riesgos de TI, de ISACA, existe un modelo de madurez para la gestión de riesgos que permite describir el estado en el que se encuentra una organización respecto de cómo se están gestionando los riesgos de TI.

El nivel 0 o no existente, es el más bajo y sencillo de describir, puesto que simplemente no hay conciencia sobre los riesgos en la organización y tampoco existe ningún control sobre ellos. No existe información estructurada y relevante sobre los riesgos, que pueda ser utilizada en la toma de decisiones. En conclusión en este nivel los riesgos no se gestionan en la empresa.

El nivel 1 o inicial. En este nivel se encuentran las empresas en donde está naciendo la conciencia acerca de los riesgos; sin embargo no existe claridad sobre el quién, cómo, cuándo y dónde se gestionan.

Se reconoce porque la gestión de riesgos de TI se visualiza como problema de carácter técnico y no se considera el valor que puede ser ganado al gestionarlos apropiadamente; además la documentación y trabajo realizado sobre los riesgos como identificación, análisis, definición de acciones de respuesta, definiciones del apetito de riesgo y el valor de tolerancia, se consideran de forma aislada en algunas actividades de TI.

El nivel 2 o repetible, se percibe cuando los procesos de gestión de riesgos tienen una tendencia al orden. Se busca cumplir con los lineamientos básicos internos de TI para responder al riesgo, aunque no se considera como objetivo realizar las acciones que permitan obtener mayor valor para la organización.

No necesariamente ha existido un nombramiento oficial dentro de la empresa para la persona o equipo que se haga responsable de gestionar los riesgos de TI, aunque sí pueden existir personas que asumen el rol. En este nivel también se cuenta con un inventario de riesgos de TI y se tienen propuestas de valores para la tolerancia al riesgo de forma aislada en las áreas internas de TI, aunque no precisamente están especificadas, evaluadas e impulsadas por el nivel directivo.

El nivel 3 o definido, se puede reconocer porque la gestión de riesgos de TI se ha dejado de ver como algo interno de TI y existe un enfoque hacia el negocio, sus procesos internos y se conoce el impacto de los riesgos existentes que conlleva el uso y la operación de los recursos de TI. También existe claridad acerca de las responsabilidades y se conoce quién es la persona que se encarga de los riesgos de TI y se conocen quienes son los responsables de los procesos en la contraparte del negocio.

Otra característica de este nivel consiste en que la información disponible sobre los riesgos ha sido comunicada por los niveles altos administrativos. Como resultado de la gestión, surgen iniciativas sobre cómo pueden aprovecharse las oportunidades de negocios y a la vez se tiene el control de mantenerse dentro de los límites de tolerancia aceptados.

El nivel 4 o gestionado, es un nivel avanzado, en el cual los procesos pueden ser dimensionados y monitoreados. Los riesgos de TI están plenamente clasificados y tienen una persona nombrada responsable de su seguimiento, además el responsable de riesgos de TI está en constante interacción con los niveles directivos y opina en las decisiones de negocio. Existe una clara y definida intervención de los niveles gerenciales y directivos, para apoyar la gestión de riesgos por medio de políticas que se han elaborado con base en los principios establecidos en el gobierno del riesgo.

La especificación del apetito de riesgo y tolerancia se conocen, son determinados y comunicados por los niveles directivos y gerenciales. Existe también claridad sobre las probabilidades de riesgo y los beneficios esperados relacionados con las actividades de TI.

El nivel 5 u optimizado, es el nivel más alto que la organización puede alcanzar. En este punto las empresas utilizan las mejores prácticas y los medios electrónicos para automatizar su funcionamiento; esto permite que los eventos puedan ser supervisados oportunamente. Existe confianza sobre cómo se gestionan los riesgos y las decisiones dentro de la organización, incluyen consideraciones sobre los riesgos de TI.

Este nivel es el óptimo para ganar valor para la organización a través de iniciativas innovadoras utilizando TI, y a su vez proteger la estabilidad de las operaciones diarias.

2.2. Alineación estratégica de TI al negocio

¿Por qué es relevante que la estrategia de TI esté alineada al negocio? Las tecnologías de la información son utilizadas por las empresas para funcionar y sobresalir en un ambiente empresarial altamente competitivo. En consecuencia, el riesgo que TI esté desalineada con los objetivos empresariales puede significar pérdidas o daños a la organización. Por ejemplo, oportunidades de negocio no aprovechadas porque los recursos de TI están siendo mal utilizados o enfocados en otras actividades.

La dirección y la gerencia de las empresas pueden tener un concepto distinto respecto de lo que TI significa para ellos y lo que esperan del mismo. Por ejemplo:

- En una perspectiva financiera y de procesos, TI puede ser vista como un área interna de la empresa que representa gastos, los cuales normalmente se tratarán de minimizar. En este contexto solamente se busca la estabilidad y disponibilidad de los sistemas; los recursos serán utilizados para alcanzar estas demandas. Las necesidades operativas son cubiertas a un nivel básico debido a la limitación de recursos y a la falta de asignación presupuestaria.

- Además de cubrir las necesidades básicas internas de las empresas, las áreas de TI pueden ser vistas y utilizadas como el medio para crear ahorros al aprovechar al máximo sus recursos y hacer eficientes los procesos operativos dentro del negocio. TI debe tener un nivel de gestión de recursos adecuado a las demandas de tiempos de respuestas y disponibilidad de los recursos y servicios por la dependencia que se ha creado.

- Además de tener cubiertas las necesidades operativas, una empresa puede pensar en crear valor según las estrategias que alcancen nuevas oportunidades de negocio, las cuales han sido impulsadas por los niveles directivos y gerenciales dentro de la organización.

La dirección y gerencia de las empresas tienen bajo su responsabilidad las decisiones estratégicas del negocio y una de ellas es determinar cuál es el papel que TI desempeñará en la organización. Cualquiera que sea el enfoque, es importante comprender que existirán objetivos con los cuales TI debe comprometerse y cumplir.

Cuando se requiere alinear estratégicamente TI al negocio, se hace necesario que las metas que se han propuesto alcanzar en el entorno corporativo estén siendo comunicadas, aceptadas y atendidas dentro de las acciones que son generadas en el plan estratégico de TI.

Esta tarea no es fácil, debido a la complejidad que se maneja internamente en la organización y en las áreas de TI. En el ambiente hay factores de complejidad, por ejemplo, tamaño del negocio, cantidad y diversidad de operaciones que la empresa realiza, cantidad de servicios que son demandados, tiempos de respuesta esperados y el tipo de negocio.

La pregunta que se presenta ahora es, ¿cómo hacer para alinear TI al negocio? Para ello se proponen las siguientes acciones:

- Obtener la información sobre cuáles son los objetivos de negocio.
- Analizar los objetivos corporativos con la finalidad de identificar la brecha existente entre cada uno de ellos y los objetivos de TI.

- Plantear los ajustes necesarios que se deben realizar para alinear los objetivos de TI con los objetivos de la organización.
- Plantear los proyectos necesarios resultantes para que los objetivos de TI estén alineados con los objetivos del negocio.

    - Esto representa estimar los costos, beneficios, tiempos y recursos necesarios.
    - Identificar los riesgos asociados, analizarlos, evaluarlos y proponer una estrategia para responder a los mismos y llevarlos al umbral de tolerancia que sea aceptable para el negocio.

- Al obtener la aprobación, establecer una comunicación constante y bilateral con el área que realiza la ejecución.
- Evaluar los resultados y comunicarlos.
- Realizar la mejora continua. Esto implica que los pasos son realizados de manera iterativa.

2.3. Identificación de riesgos

La identificación de riesgos es la parte inicial de un conjunto de actividades que se realizará para llegar a obtener el portafolio de riesgos de la organización.

Para alcanzar este objetivo, es importante que en la empresa exista claridad sobre la unificación de criterios acerca de los riesgos de TI y los corporativos. Esto se logra promoviendo una cultura organizacional que involucre a las personas y que informe oportunamente acerca de los eventos relacionados a los riesgos, el impacto que estos pueden tener en la organización, los criterios definidos para el apetito de riesgo, la tolerancia de los mismos, las políticas, procedimientos y acciones para responder a los riesgos.

¿Qué debemos hacer para identificar los riesgos? La actividad inicial consiste en determinar cuáles son los escenarios de riesgos que pueden ocurrir dentro de la organización y cuáles son los pasos que permitirán recolectar toda la información que se necesita.

Según el marco de trabajo de riesgos de TI, de ISACA, a continuación se describen los pasos a seguir:

- Especificar el modelo que permita colectar y organizar la información obtenida. Este modelo debe estar basado en las técnicas y normas de riesgo, integradas dentro de la empresa. El modelo debe incluir lo siguiente:

    - Actividad de negocio.
    - Valores esperados por la organización.
    - Activos o recursos empresariales involucrados.
    - Tipos de evento. Es necesario clasificar la información de riesgos de acuerdo con los tipos de eventos que se están generando. Por ejemplo eventos de pérdida o eventos que den muestra de vulnerabilidades.
    - Especificación de actores involucrados.

- Especificación de los criterios acerca de cómo puede influir el factor tiempo.
- Indicación sobre cómo se puede afectar la probabilidad e influir en los factores de riesgos como el impacto, frecuencia y magnitud. Representarlos en forma cualitativa y cuantitativa.
- Especificación del valor que se puede ganar.
- Descripción sobre la forma para obtener mediciones y la unidad de medida que se va a utilizar.
- Especificación del apetito y la tolerancia al riesgo.
- Especificación de las obligaciones adquiridas por la empresa en un contexto interno o externo.
  - ✓ Descripción de la forma sugerida de respuesta al riesgo cuando se presente.
  - ✓ Descripción sobre la manera de comunicar o informar.

- Obtener información del entorno empresarial
  - Consultar los diferentes orígenes de datos dentro de la empresa, las diferentes áreas de negocio y de cumplimiento interno y entidades que regulan el cumplimiento externo y legal y el entorno político.
  - Consultar los objetivos estratégicos de la organización, las políticas y normas internas y especificaciones de los productos.
  - Obtener información sobre los riesgos que generalmente ocurren, y los datos acerca de riesgos frecuentes de acuerdo con estudios previos.
  - Obtener información acerca de los eventos históricos tanto internos como externos. Hay que aprender de las experiencias que ha dejado el pasado aunque no correspondan con vivencias propias.

- Obtener información por medio de la experiencia y conocimiento de las personas, tomando en consideración las causas que han originan los hechos.
- Consultar también otras fuentes de información concernientes a la naturaleza del negocio.
- Obtener información acerca de las tendencias del mercado, la industria y la competencia.
- Consultar información sobre las capacidades que tiene TI en la organización, sus operaciones y controles internos.

- Identificar eventos del riesgo. La información puede ser estructurada con base en la observación detallada de los eventos que han surgido y que pueden influir en el impacto y afectar el valor obtenido en el uso y operación de la TI.

- Identificar factores de riesgos. Al analizar los eventos se debe considerar cuales fueron los factores que influyeron en la frecuencia, impacto y magnitud.

2.4. Analizar y mantener un perfil de riesgos

La actividad de análisis de riesgos es amplia, depende de la necesidad que la ha originado y del nivel de madurez que la empresa presente. Según el marco de trabajo de riesgos de TI, de ISACA, a continuación se describen los pasos para su realización:

- Para iniciar, se debe considerar el alcance de lo que se desea obtener del proceso o actividad de negocio, el valor o los valores óptimos esperados y disponer de la información recogida durante la identificación de riesgos.

- Efectuar el análisis de los escenarios de riesgo. En esta actividad se utiliza la toda la información colectada durante el proceso inicial y se busca alcanzar los siguientes tres objetivos:

    - Estimar los umbrales del valor máximo de perjuicio para la organización y los límites donde inicia la generación del valor para la organización.
    - Determinar los controles, las mediciones que se hacen indispensables y las acciones requeridas, para dar una adecuada atención al riesgo. A ello se debe agregar la estimación del costo y ser comparado con el valor que representa aceptarlo, si se materializa.
    - Determinar en qué punto los controles y las acciones que se deben tomar, permiten que el riesgo residual alcance la zona de valores aceptados en cuanto a la tolerancia y apetito de riesgo.

- Como resultado del análisis se debe considerar las posibles respuestas a los riesgos y las que sean factibles de implementar. Las opciones son: evitarlos, compartirlos, transferirlos, reducirlos o mitigarlos, explotarlos y aceptarlos. Cada una representa recursos y costos distintos, los cuales pueden ser identificados para tomar la mejor decisión. Se debe considerar que además del costo, se hace indispensable tomar en cuenta los factores de cumplimiento.

El resultado de este análisis se adjunta al perfil de riesgos corporativos existentes, el cual debe ser creado, mantenido y actualizado en forma continua. Además, puede ser utilizado para reunir información cruzada entre los procesos de negocio y los riesgos de TI.

Según el modelo GRC, para crear un perfil de procesos y riesgos se hace necesario realizar lo siguiente:

- Creación de un mapa de procesos de negocio y recursos de TI. Este recurso facilitará en forma contextual, una visión rápida de la dependencia que tiene el negocio de TI.
- Incluir los procesos internos de TI.
- Especificar puntos críticos sobre recursos y procesos del negocio, estimar de acuerdo con los niveles de servicio esperados, los recursos que son necesarios para ello.
- Indicar la información relevante para el análisis de riesgos como los actores, el involucramiento del factor tiempo, el tipo de amenaza, recursos del negocio utilizados y el impacto resultante.

2.5. Respuesta a riesgos

Teniendo disponible la identificación, el análisis y el perfil de riesgos de TI, conviene ahora preparar la respuesta que se traduce en las acciones que tienen como objetivo llevar el riesgo inherente hacia un riesgo residual, que sea aceptado por el negocio de acuerdo con los parámetros de apetito y tolerancia definidos.

De acuerdo con el marco de trabajo de riesgos de TI, de ISACA y el artículo sobre análisis de riesgos en el portal de revistas peruanas, para planificar la respuesta a los riesgos, a continuación se describen las diferentes estrategias que pueden ser asumidas:

- Aceptarlos: esto involucra que hay disposición de recibir la consecuencia del riesgo a pesar de que se conoce y se tiene conciencia del impacto para la organización y a pesar de ello estar de acuerdo en asumirlo. En este contexto, se puede especificar qué persona o área de negocio puede asumir el riesgo.

- Transferirlos: esta estrategia implica que la responsabilidad y la acción de asumir la consecuencia del riesgo es asimilado por terceros. La forma más común de implementar esta estrategia es por medio de aseguradoras.

- Compartirlos: es una estrategia similar a la anterior, porque se involucra a un tercero y de acuerdo con convenios entre las partes, se asume entre ambos la consecuencia del riesgo. Por ejemplo, al subcontratar a un tercero para la ejecución de un proyecto, se puede convenir penalizaciones por incumplimiento del tiempo de entrega. En este ejemplo, la organización asume el impacto de no tener en tiempo los beneficios que el proyecto les produce.

- Reducirlos: las acciones que son tomadas para reducir o mitigar el riesgo están enfocadas en influir en que su frecuencia o impacto sea menor, hasta que alcance el nivel aceptado por el negocio. La clave está en identificar los eventos y factores involucrados y tomar acciones correctivas.

- Explotarlos: significa que los eventos que apoyen la generación del valor sean forzados a que ocurran.

- Mejorarlos: puede ocurrir cuando se hacen ajustes y se influye en los eventos que permitan mejorar la oportunidad de generar valor y que el beneficio para la organización sea mayor.

- Evitarlos: esta acción debe ser realizada como último recurso, cuando las otras estrategias no son factibles de implementar o tienen un impacto mayor al que la organización está dispuesta a asumir para responder al riesgo. Para evitar los riesgos básicamente hay que desistir de la actividad que se desea hacer o suprimir sus causas.

Es necesario hacer ver que en algunos casos puede existir más de una respuesta a los riesgos que puede ser implementada, entonces se debe analizar otros factores que pueden ser considerados y que ayudarán en la toma de decisiones para que sea elegida la que represente mayor beneficio a la empresa; para comprenderlos se debe encontrar respuesta a las siguientes interrogantes:

- ¿Cuánto cuesta implementar la estrategia de respuesta al riesgo? La realización de actividades de respuesta implica el uso de los recursos de la organización o de terceros los cuales deben ser cuantificados en términos económicos y el tiempo requerido.

- ¿Qué tan significativo es el impacto en la organización? Esto puede responderse al observar los factores de riesgos relacionados con el impacto, frecuencia y magnitud.

- ¿Está preparada la empresa para asumir la implementación de la estrategia de riesgos? Hay que evaluar si la empresa está preparada internamente para responsabilizarse por realizar las actividades que

implican la respuesta al riesgo y ver si sus recursos personales y de infraestructura colaboran o agregan resistencia para su implementación.

- ¿Qué tanto impacta la estrategia en el resultado final? Es importante determinar si la estrategia elegida como solución sea muy probable y efectiva en los resultados que promete obtener.

Al considerar estos factores, la respuesta a los riesgos puede clasificarse de acuerdo con los resultados que se obtendrán y maximizar los beneficios para la organización.

2.6. Decisiones del negocio

Hasta ahora se tiene disponible la identificación de los riesgos, un análisis sobre ellos, el perfil de riesgos de TI y definición sobre cómo será la respuesta. Las decisiones de negocio deben estar orientadas al aprovechamiento de las oportunidades que son generadas al utilizar TI considerando su capacidad y los riesgos relacionados. Para presentar a los encargados de la toma de decisiones, según el marco de trabajo de riesgos de TI, de ISACA, puede elaborarse un informe que tenga las siguientes características:

- Descripción general de los procesos, activos o recursos de la organización, recursos de TI, alcances especificados, presentación de escenarios de riesgos y oportunidades.
- El informe debe tener también información en perspectiva cuantitativa económica, que incluya los rubros de magnitudes, pérdida y probabilidad.
- Incluir las actividades necesarias para controlar y gestionar el riesgo y los valores cuantitativos correspondientes.

- Incluir también información en perspectiva cualitativa y cuantitativa; si las oportunidades generadas son alcanzadas, se debe incluir los rubros de magnitudes de ganancia y probabilidad.

Las personas encargadas de la toma de decisiones deberán recibir este informe y ser asesorados por el responsable de riesgos de TI, quien podrá apoyarles para resolver dudas y ayudarles con la comprensión de los elementos técnicos relacionados.

Se debe tomar en cuenta que el informe puede ser rechazado por las personas que toman decisiones, para cambiar el alcance del análisis, para modificar algunas características propias del negocio o para incluir cambios en las capacidades de TI, lo cual implicaría realizar nuevamente el análisis de riegos considerando estos cambios.

2.7. Controles

Los niveles directivos y gerenciales tienen la responsabilidad de tomar las decisiones sobre las estrategias de negocio que implementarán para cumplir los objetivos organizacionales. Para tener una certeza razonable que se van a alcanzar, se pueden apoyar en la gestión de riesgos y así obtener el máximo beneficio.

Al tomar decisiones sobre cuáles son las estrategias que van a implementar para responder a los riesgos, nace la necesidad de asegurar que tales acciones se realicen en forma oportuna. Para ello es necesario diseñar e implementar controles que contribuyan a su cumplimiento.

Según COSO ERM, las actividades de control deben ser traducidas a reglamentos internos como normativas, políticas y procedimientos. En algunos casos estos controles son manuales o pueden estar incluidos en los sistemas de información que han sido implementados.

Los controles pueden generar información en forma de alertas que notifiquen un evento que sea de relevancia para la respuesta a los riesgos, pues al ocurrir algunos eventos, estos pueden influenciar en la materialización de un riesgo o una oportunidad de negocio, la cual debe ser tratada de acuerdo con la especificación de respuesta a los riesgos previamente establecida.

En las actividades de control se requiere supervisión, debido a que los lineamientos y procedimientos de negocio pueden ser omitidos en algún momento.

2.8. Gestión de la comunicación

La comunicación es un factor clave en la correcta gestión de riesgos de la organización. La comunicación efectiva permite que las partes interesadas, desde los puestos directivos, gerencias y personal operativo, sea permeado por la cultura de riesgos. Por el contrario, al existir una comunicación inadecuada, se puede generar falta de interés en las políticas y procedimientos destinados a gestionar los riesgos, además de que existan muchas fallas en los procesos debido a incumplimientos por ignorancia o por falta de interés.

La comunicación, consiste en compartir información y asegurar la comprensión del mensaje entregado. No siempre se debe realizar con matices de formalidad, sin embargo, de acuerdo con el marco de trabajo de riesgos de TI, de ISACA, es necesario que cumpla con algunas características que son aplicables en la administración de riesgos:

- Tener claridad: el mensaje debe ser sencillo y fácil de comprender. Es útil conocer la audiencia del mensaje, para incluir el nivel de detalle acorde a sus intereses y responsabilidades.
- Se debe dar a conocer en el momento oportuno: el mensaje debe ser entregado en el momento adecuado. Para gestionar un riesgo, el factor tiempo es importante, pues un mensaje fuera de tiempo puede implicar que el riesgo se materialice y alcance su máximo impacto.
- Ser directo: la información no debe saturar a sus receptores.
- Receptores correctos: consiste simplemente en dirigir los mensajes a las personas que deben estar informadas.

Durante la gestión de riesgos de TI, la información es preparada y organizada, generando diferentes flujos de comunicación.

Entonces, surgen las siguientes interrogantes: ¿Qué se debe comunicar y a quién? Para responder la primera de ellas se tiene, por ejemplo: políticas, procedimientos, informes sobre identificación, análisis, evaluación de riesgos e información histórica de eventos ocurridos que han conducido a la materialización de riesgos. Para responder a la segunda interrogante, se debe considerar los diferentes grupos receptores y generadores de información de acuerdo con su responsabilidad y su audiencia objetivo, como se puede observar en la Tabla I que se presenta a continuación:

Tabla I. **Matriz de gestión de la comunicación**

Responsables	**¿De qué es responsable?**	**¿Quién debe estar informado?**
Dirección y gerencias	Estrategia de riesgos	Todos los empleados
Dirección y gerencias	Objetivos organizacionales	Todos los empleados
Dirección y gerencias	Especificaciones cultura de riesgo	Todos los empleados
Dirección y gerencias	Políticas, procedimientos	Todos los empleados
Responsable de TI	Capacidades de TI	Dirección y gerencias
Responsable de riesgos, propietario de procesos, personal especializado TI	Identificar riesgos	Dirección y gerencias
Responsable de riesgos, propietario de procesos, personal especializado TI	Análisis de riesgos y evaluación	Dirección y gerencias
Responsable de riesgos, propietario de procesos, dirección y gerencias	Perfil del riesgo y portafolio de riesgos	Dirección y gerencias, personal especializado TI
Responsable de riesgos, propietario de procesos	Respuesta de riesgos	Dirección y gerencias
Dirección y gerencias	Informe sobre decisiones sobre las respuestas a riesgos a ejecutar	Responsable de riesgos, propietario de procesos, personal especializado TI
Responsable de riesgos	Informes de actividades de control de riesgos	Dirección y gerencias, propietario de procesos, personal operativo negocio, personal especializado TI
Responsable de riesgos	Historia y documentación de eventos de riesgos materializados	Dirección y gerencias, propietario de procesos, personal operativo negocio, personal especializado TI

Fuente: Risk-IT-framework,http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-framework-spanish.pdf

3. PRINCIPALES ESCENARIOS DE RIESGOS EN TI

La creación de los escenarios de riesgos es la técnica que permite describir los riesgos mediante eventos que involucran a actores, tipos de amenazas y el efecto del tiempo. Al tenerlos concluidos, son utilizados en la fase de análisis de riesgos para calcular el impacto, magnitud y frecuencia.

Para estimar los escenarios de riesgo en una organización se recomienda dos perspectivas: primero, se sugiere considerar su estudio tomando como base los objetivos de negocio. Segundo, se hace con base en un listado genérico de riesgos. Ambas perspectivas tienen sus ventajas y desventajas; por ejemplo, la primera manera permite desde el inicio alinearse con los objetivos de negocio y apoyar su cumplimiento aunque podría omitir algunas situaciones básicas. Por el otro lado, la segunda manera consiste en una lista de escenarios de riesgo genéricos que permiten tener un punto de partida con información disponible para ser analizada y se complementa verificando que se cumplan todos los objetivos de negocio.

De acuerdo con el marco de trabajo de riesgos de TI, de ISACA, a continuación se describirá un listado de escenarios de riesgos donde se cubre aspectos generales de TI. Esta lista no pretende suprimir la identificación de los mismos dentro de cualquier organización, debido a que cada una tiene circunstancias particulares que deben ser consideradas, pero si puede utilizarse como una guía.

Cada escenario describe al actor, el tipo de amenaza, el evento, el activo o recurso, los riesgos, la oportunidad y cuáles son los factores que reducen o amplifican la probabilidad e impacto. Si algún factor no se presenta es porque se considera poco relevante o no existente en el escenario.

3.1. Escenarios de riesgos de infraestructura física de TI

En el contexto de infraestructura física de TI se considerarán todos los componentes de hardware tales como: servidores, computadoras de escritorio, dispositivos móviles, laptops, dispositivos de comunicaciones, instalaciones, etc.

3.1.1. Obsolescencia de la infraestructura física

- Actores: personal interno responsable.
- Tipo de amenaza: falla.
- Evento: diseño y estrategia inapropiada respecto de la infraestructura.
- Activo o recurso TI: componentes físicos de la infraestructura.
- Riesgo: la obsolescencia del hardware no permitirá satisfacer nuevos requerimientos de negocio que utilicen mayor capacidad.
- Riesgos positivos u oportunidades: con infraestructura moderna se puede soportar el crecimiento de operaciones, uso de nuevas tecnologías y soporte para uso de software moderno.
- Factores de impacto alto: el entorno tecnológico cambiante, importancia estratégica de TI, capacidad interna de TI y gestión adecuada de riesgos.
- Factores de impacto medio: complejidad del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y la detección de sus consecuencias puede ser largo, asimismo al ocurrir el efecto, puede ser de larga duración.

3.1.2. Daño o destrucción de la infraestructura física

- Actores: personal interno o personal externo, la naturaleza.
- Tipo de amenaza: acción de la naturaleza, accidentes, acción malintencionada.
- Evento: daño o destrucción.
- Activo o recurso TI: componentes físicos de la infraestructura.
- Riesgos: pérdida temporal o permanente de parte de la infraestructura física. Además, pérdida de información almacenada. Interrupción en la continuidad del servicio, dependiendo de qué parte de la infraestructura se dañe.
- Factores de impacto alto: la importancia estratégica de TI, la situación geográfica y política del país.
- Factor tiempo: el tiempo que transcurre entre el evento y las consecuencias, es inmediato; al ocurrir el efecto del riesgo, puede ser de larga duración.

3.1.3. Robo a la infraestructura física

- Actores: personal interno o externo.
- Tipo de amenaza: acción malintencionada.
- Evento: robo.
- Activo o recurso TI: componentes físicos de la infraestructura.
- Riesgos: pérdida de algún componente de la infraestructura física. Puede involucrar pérdida de información almacenada. También pérdida de la continuidad del servicio, dependiendo de qué parte de la infraestructura sea robada.

- Factores de impacto alto: la importancia estratégica de TI, gestión adecuada de riesgos, la situación geográfica y política del país.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto, al ocurrir el efecto del riesgo, puede ser de larga duración.

3.1.4. Arquitectura inadecuada de la infraestructura física

- Actores: personal interno responsable.
- Tipo de amenaza: error o funcionamiento inadecuado.
- Evento: diseño y estrategia inapropiada.
- Activo o recurso TI: componentes físicos de la infraestructura.
- Riesgos: sub utilización de la infraestructura, incumplir la expectativa de retorno de la inversión, pérdida de oportunidades de otra inversión, pérdida de flexibilidad y agilidad por mal diseño. También es posible que la capacidad resulte inadecuada e insuficiente para crecimiento.
- Riesgos positivos u oportunidades: con un buen diseño y evaluación de las inversiones, la infraestructura puede ser utilizada óptimamente.
- Factores de impacto alto: capacidad para administrar TI, capacidad de TI, importancia estratégica de TI y complejidad del negocio.
- Factores de impacto medio: la situación económica, el entorno tecnológico.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es largo; al ocurrir el efecto del riesgo, puede ser también de larga duración.

3.1.5. Instalación y cambios de la infraestructura física

- Actores: personal interno, personal externo o proveedores.
- Tipo de amenaza: falla.
- Evento: acción malintencionada o accidental.
- Activo o recurso TI: componentes físicos de la infraestructura.
- Riesgos: configuración incorrecta o faltante ante un cambio o instalación de hardware, puede ocasionar fallas en la infraestructura y en la continuidad del servicio según qué parte de la infraestructura esté involucrada.
- Factores de impacto alto: importancia estratégica de TI y complejidad del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto. La duración es variable y depende de la disponibilidad de recursos humanos o de hardware. El momento en que ocurre puede afectar las operaciones en lapsos de tiempo críticos para la organización.

3.2. Escenarios de riesgos con el personal

Se hace mención a personas que laboran internamente en cualquier área de TI en toda su estructura organizacional.

3.2.1. Ausencia del personal de TI

- Actores: personal interno de TI.
- Tipo de amenaza: falla.
- Evento: ejecución administrativa inadecuada y ocurrencia de problemas con el personal.

- Activo o recurso TI: personal interno de TI.
- Riesgos: ausencia temporal o definitiva de personas clave dentro de TI y la dificultad o imposibilidad de contratar personal permanente o temporal.
- Factores de impacto alto: la competencia, situación geográfica y política del país, importancia estratégica de TI, capacidad de TI, capacidad para administrar TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la complejidad del negocio, situación económica y el entorno tecnológico cambiante.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede ser corto a mediano plazo. La duración puede ser moderada y el momento en que ocurre puede afectar el resultado de las actividades en las cuales el personal tenga responsabilidad directa.

3.2.2. Falta de habilidades y experiencia del personal de TI

- Actores: personal interno de TI.
- Tipo de amenaza: falla.
- Eventos: definición de la estrategia de desarrollo personal y diseño de la estructura organizacional inadecuados.
- Activo o recurso TI: personal interno de TI.
- Riesgos: falta de conocimiento especializado de TI, falta de comprensión y entendimiento del negocio. Esto podría repercutir en el desaprovechamiento de la tecnología y los recursos de TI en soluciones mal diseñadas.
- Riesgos positivos u oportunidades: si se tiene el personal capacitado y adecuado, se incrementa la posibilidad de crear valor para la organización por medio de trabajos bien ejecutados, servicios bien diseñados y con la funcionalidad esperada.

- Factores de impacto alto: la competencia, la situación geográfica y política del país, importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la complejidad del negocio, la situación económica y el entorno tecnológico cambiante.
- Factor tiempo: el tiempo que transcurre entre los eventos y su detección es de corto plazo. La duración puede ir de moderada a largo plazo.

3.2.3. Insuficiencia de personal especializado de TI

- Actores: personal administrativo interno de TI.
- Tipo de amenaza: falla.
- Evento: definición de la estrategia de gestión de personal y diseño de la estructura organizacional inadecuadas.
- Activo o recurso TI: personal interno de TI.
- Riesgos: baja calidad, retrasos en la entrega de soluciones y servicios
- Riesgos positivos u oportunidades: al disponer de la cantidad de recurso humano capacitado y acorde a las necesidades de la organización, se puede responder a las necesidades con mayor calidad y prontitud.
- Factores de impacto alto: la competencia, importancia estratégica de TI, capacidad de TI, capacidad para administrar TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la complejidad del negocio, la situación económica y el entorno tecnológico cambiante.
- Factor tiempo: el tiempo que transcurre entre los eventos y su detección es de corto plazo. La duración puede ir de moderada a largo plazo. El momento en el que ocurren los eventos puede ser importante debido a las necesidades presentes para la organización.

3.3. Escenarios de riesgos de gestión de proyectos

3.3.1. Proyectos no finalizados

- Actores: personal interno involucrado en el proyecto.
- Tipo de amenaza: falla.
- Evento: falla en la ejecución del proyecto.
- Activo o recurso TI: grupo de proyectos.
- Riesgos: proyectos no finalizados, debido a cambios de prioridades del negocio, falta de apoyo administrativo, falta de participación de las partes interesadas en el proyecto, recursos no disponibles y como consecuencia se haya tenido retrasos consistentemente.
- Riesgos positivos u oportunidades: los proyectos se han suspendido o cancelado oportunamente debido a cambios en prioridades o estrategias de negocio o porque ya no aportan los beneficios ante cambios en el entorno.
- Factores de impacto alto: la situación económica, la importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI, la gestión adecuada de riesgos y la complejidad del negocio.
- Factores de impacto medio: la competencia.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es de corto plazo o de inmediato. La duración de los efectos puede ser moderada o a largo plazo. El momento en el que ocurren los eventos puede ser muy importante debido a las necesidades, expectativas y compromisos de la organización.

3.3.2. Riesgos económicos del proyecto

- Actores: personal interno involucrado en el proyecto.
- Tipo de amenaza: falla.
- Evento: falla en la gestión del proyecto en aspectos económicos.
- Activo o recurso TI: grupo de proyectos.
- Riesgos: superación del presupuesto asignado en forma aislada o recurrente en otros proyectos. Falta de una perspectiva y control económico del proyecto.
- Riesgos positivos u oportunidades: los proyectos se realizan dentro del presupuesto asignado.
- Factores de impacto alto: la competencia, la importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI, la gestión adecuada de riesgos.
- Factores de impacto medio: la situación económica, la complejidad del negocio y el entorno tecnológico cambiante.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es de corto o mediano plazo. La duración de los efectos puede ser a mediano o largo plazo.

3.3.3. Retraso en entrega de proyectos

- Actores: personal interno involucrado en el proyecto y terceros.
- Tipo de amenaza: falla.
- Evento: falla en la gestión del proyecto.
- Activo o recurso TI: grupo de proyectos.

- Riesgos: retraso en la entrega de proyectos realizados por personal interno o por personal externo en la modalidad de *outsourcing*, debido a cambios de prioridades del negocio, falta de apoyo administrativo, falta de participación de las partes interesadas en el proyecto, recursos no disponibles, constantes cambios en el alcance del proyecto, utilización de la tecnología inadecuada o no probada.
- Riesgos positivos u oportunidades: ejecución de proyectos en el tiempo establecido.
- Factores de impacto alto: la competencia, situación económica, importancia estratégica de TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la capacidad de TI y la de administrar TI.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es de corto o mediano plazo. La duración de los efectos puede ser a mediano o largo plazo.

3.3.4. Baja calidad en los proyectos

- Actores: personal interno involucrado en el proyecto y terceros.
- Tipo de amenaza: falla.
- Evento: falla en la administración y ejecución del proyecto.
- Activo o recurso TI: grupo de proyectos.
- Riesgos: falta de calidad en los entregables del proyecto. Documentación faltante o desactualizada, funcionalidad incompleta o diferente a la requerida, o con errores.
- Riesgos positivos u oportunidades: los entregables cumplen con los requisitos del proyecto.
- Factores de impacto alto: la competencia, importancia estratégica de TI y la gestión adecuada de riesgos.

- Factores de impacto medio: la capacidad de TI y la de administrar TI, el entorno regulatorio y legal del país.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es de corto o mediano plazo. La duración de los efectos puede ser a mediano o largo plazo. El momento en el que ocurren los eventos puede ser muy importante, debido a que problemas de calidad en la fase final del proyecto pueden afectarlos significativamente.

3.3.5. Falta de visión de programa de proyectos

- Actores: personal administrativo interno.
- Tipo de amenaza: falla.
- Evento: falla en la definición de la estrategia de TI.
- Activo o recurso TI: grupo de proyectos.
- Riesgos: falta estrategia corporativa y falta de visión del portafolio o grupo de proyectos. Desaprovechamiento de los recursos de TI en proyectos no relevantes y pérdida de oportunidades para el negocio.
- Riesgos positivos u oportunidades: elaborar programas corporativos que contengan proyectos que apoyen los objetivos estratégicos de la organización.
- Factores de impacto alto: la importancia estratégica de TI, complejidad del negocio, capacidad de cambio del negocio, capacidad de TI, capacidad para administrar TI y para administrar los riesgos en la organización.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es de mediano o largo plazo y la duración de los efectos también puede ser a mediano o largo plazo.

3.4. Escenarios de riesgos en la gestión de la seguridad

3.4.1. Ataque lógico a la seguridad

- Actores: personal interno o externo.
- Tipo de amenaza: acción malintencionada.
- Evento: uso inapropiado y diseño inefectivo.
- Activo o recurso TI: información del negocio, servicios disponibles y aplicaciones del negocio.
- Riesgos: ataque por medio de virus, intento de ingreso a los sistemas por personas no autorizadas con el objetivo de dejar indispuestos los servicios, alterar la configuración de aplicaciones en la web y espionaje industrial.
- Factores de impacto alto: la situación geográfica y política, el entorno regulatorio y legal del país, la importancia estratégica de TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la capacidad de TI, complejidad del negocio y la capacidad de administrar TI.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es de corto o mediano plazo.

3.4.2. Traspasar la seguridad

- Actores: personal interno o externo.
- Tipo de amenaza: acción malintencionada.
- Evento: uso inapropiado y diseño inefectivo de mecanismos de defensa para las redes y para los accesos físicos de TI.
- Activo o recurso TI: información del negocio.

- Riesgos: esquivar la seguridad de accesos, obtener información sin autorización con fines ilícitos, extracción o robo de información sensible.
- Factores de impacto alto: la importancia estratégica de TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la situación geográfica y política, el entorno regulatorio y legal del país, la capacidad de TI, complejidad del negocio y la capacidad de administrar TI.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede alcanzar el mediano plazo.

3.4.3. Alteración de la integridad de la información

- Actores: personal interno o externo.
- Tipo de amenaza: falla y acción malintencionada.
- Evento: modificaciones malintencionadas o erróneas.
- Activo o recurso TI: infraestructura física, de servicios y aplicaciones.
- Riesgos: alteración intencional de datos de configuración, datos del negocio, información sensible de los clientes o proveedores; todo ello con el fin de cometer un acto ilícito.
- Factores de impacto alto: la competencia, importancia estratégica de TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la capacidad de TI, la capacidad de administrar TI y el entorno regulatorio y legal del país.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede ser corto o mediano plazo y la duración de los efectos puede alcanzar el largo plazo.

3.4.4. Riesgos a la exposición de la información

- Actores: personal interno o externo.
- Tipo de amenaza: acción malintencionada o accidental.
- Evento: uso inapropiado, incumplimiento o por accidente.
- Activo o recurso TI: información sensible para el negocio.
- Riesgos: el personal con los accesos a la información puede exponer información a terceras personas, ajenas a la institución, utilizando los medios autorizados por la organización, por ejemplo: ante el uso descuidado, accidental o malintencionado de dispositivos móviles, laptops, correo electrónico, compartir información en redes sociales, etc.
- Factores de impacto alto: la importancia estratégica de TI y la gestión adecuada de riesgos.
- Factores de impacto medio: la situación geográfica y política, el entorno regulatorio y legal del país y la capacidad de administrar TI.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede alcanzar el largo plazo.

3.5. Riesgos en las aplicaciones

3.5.1. Decisiones de inversión en aplicaciones

- Actores: personal administrativo interno.
- Tipo de amenaza: falla.
- Evento: diseño inefectivo de la estrategia de TI para asesorar al negocio en inversiones de TI.
- Activo o recurso TI: aplicaciones.

- Riesgos: falta de involucramiento de parte del personal de TI en la toma de decisiones de inversión relacionadas con TI de parte del negocio. Se puede perder la perspectiva de aprovechamiento de la tecnología y la adecuada gestión con la implementación de sistemas respecto de los otros proyectos en curso y su debida priorización.
- Riesgos positivos u oportunidades: se obtiene mejores resultados con el uso de nuevas tecnologías y mejor aprovechamiento de la inversión.
- Factores de impacto alto: la importancia estratégica de TI, complejidad del negocio, capacidad de cambio del negocio, capacidad para administrar los riesgos, entorno regulatorio y legal del país, entorno tecnológico que cambia constantemente, competencia y la situación económica.
- Factores de impacto medio: la capacidad de TI y su administración.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede ser mediano plazo y la duración de los efectos puede alcanzar el largo plazo.

3.5.2. Envejecimiento de las aplicaciones de negocio

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: falla de diseño o elección al adquirir aplicaciones.
- Activo o recurso TI: aplicaciones del negocio.
- Riesgos: envejecimiento de las aplicaciones. Implica uso de tecnología antigua, alto costo para mantenimiento, dificultad de integración con tecnología nueva, documentación inexistente o desactualizada.
- Riesgos positivos u oportunidades: las aplicaciones o sistemas de información con tecnología moderna se pueden integrar a los procesos de negocio con mayor facilidad.

- Factores de impacto alto: la situación económica, entorno tecnológico que cambia constantemente, importancia estratégica de TI, capacidad de cambio del negocio y capacidad para administrar los riesgos.
- Factores de impacto medio: la competencia, la capacidad de TI, la capacidad administrar TI y la complejidad del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede ser mediano o largo plazo, mientras que la duración de los efectos puede alcanzar el largo plazo.

3.5.3. Implementación inadecuada de las aplicaciones

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: falla de ejecución al implementar aplicaciones.
- Activo o recurso TI: aplicaciones del negocio.
- Riesgos: errores detectados en la aplicación cuando ha sido liberada para uso. Errores por mal uso de la aplicación por falta de entrenamiento y desaprovechamiento de las nuevas funcionalidades de software. Además, riesgos en la preparación de la configuración e instalación de las aplicaciones en ambientes productivos.
- Factores de impacto alto: la importancia estratégica de TI y la capacidad para administrar los riesgos.
- Factores de impacto medio: la situación económica, capacidad de TI, capacidad administrar TI, la complejidad del negocio y la capacidad de cambio del negocio.

- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto plazo y la duración de los efectos puede ser de corto plazo si se acciona de inmediato; sin embargo, el tiempo en el que ocurre el evento es crucial si la aplicación es crítica para el negocio.

3.5.4. Inestabilidad de las aplicaciones

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: diseño inadecuado.
- Activo o recurso TI: aplicaciones del negocio.
- Riesgos: errores intermitentes en aplicaciones importantes para la organización y fallas de funcionalidad en las aplicaciones que son críticas para la organización.
- Factores de impacto alto: la importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI y los riesgos.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto plazo y la duración de los efectos puede ir del corto al mediano plazo; sin embargo el tiempo en el que ocurre el evento es crucial si la aplicación es crítica para el negocio.

3.5.5. Falta de capacidad en las aplicaciones

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: diseño inadecuado.
- Activo o recurso TI: aplicaciones del negocio.

- Riesgos: los sistemas de información responden ineficientemente cuando son exigidos con mayor cantidad de operaciones o cuando nuevas aplicaciones son adheridas.
- Factores de impacto alto: la importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI y los riesgos.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto plazo y la duración de los efectos puede ir del mediano al largo plazo; sin embargo el tiempo en el que ocurre el evento es crucial si la aplicación es crítica para el negocio.

3.5.6. Envejecimiento de aplicaciones de infraestructura

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: diseño inadecuado.
- Activo o recurso TI: aplicaciones que sirven para el funcionamiento de la infraestructura.
- Riesgos: las versiones instaladas de los sistemas operativos y software de base de datos ya no son soportadas por sus proveedores.
- Factores de impacto alto: el entorno tecnológico que cambia constantemente, la importancia estratégica de TI, la capacidad de TI y la capacidad para administrar los riesgos.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es mediano plazo y la duración de los efectos también puede ser a mediano plazo.

3.5.7. Aplicaciones intrusas

- Actores: personal interno y externo.
- Tipo de amenaza: actos malintencionadas o accidentales.
- Evento: diseño inadecuado.
- Activo o recurso TI: servidores, laptops, computadoras personales de escritorio y otros dispositivos.
- Riesgos: ingreso de software malicioso a servidores y equipos de la organización.
- Factores de impacto alto: el entorno regulatorio y legal del país, la importancia estratégica de TI y la capacidad para administrar los riesgos.
- Factores de impacto mediano: la competencia y la situación geográfica y política.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección puede ser corto, mediano o largo plazo y la duración de los efectos puede alcanzar el mediano plazo.

3.6. Riesgos en soporte y entrega de servicios

3.6.1. Riesgos en soporte y entrega de servicios

- Actores: personal interno, personas externas o proveedores.
- Tipo de amenaza: falla.
- Evento: diseño inadecuado.
- Activo o recurso TI: portafolio de servicios de TI.

- Riesgos: el soporte y servicios que son provistos por proveedores o personal interno no alcanza los niveles de servicio requeridos. También el rendimiento del personal que trabaja bajo la modalidad de *outsourcing* puede alcanzar niveles inadecuados de productividad. Otro riesgo inherente es la pérdida de confianza hacia TI.
- Factores de impacto alto: la situación económica, competencia, situación geográfica y política, el entorno regulatorio y legal del país, el entorno tecnológico que cambia constantemente, la importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI, la complejidad del negocio y la capacidad para administrar los riesgos.
- Factores de impacto medio: la capacidad de cambio del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto. La duración de los efectos puede alcanzar el corto o mediano plazo.

3.6.2. Riesgos en rendimiento de los servicios

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: interrupción de los servicios.
- Activo o recurso TI: portafolio de servicios de TI.
- Riesgos: fallas continuas o extendidas en los servicios.
- Factores de impacto alto: la situación económica y la importancia estratégica de TI.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto. La duración de los efectos puede alcanzar el corto o mediano plazo.

3.7. Riesgos en cumplimiento corporativo

3.7.1. Riesgos en cumplimientos de acuerdos y compromisos

- Actores: personal interno y externo.
- Tipo de amenaza: falla, eventos malintencionados.
- Evento: ejecución inadecuada.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: obligaciones adquiridas con proveedores o clientes que no son cumplidas.
- Factores de impacto alto: la competencia, situación geográfica y política, el entorno regulatorio y legal del país, la importancia estratégica de TI, capacidad de TI, capacidad para administrar TI, complejidad del negocio y la capacidad para administrar los riesgos.
- Factores de impacto medio: el entorno tecnológico que cambia constantemente y capacidad de cambio del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto o mediano plazo. La duración de los efectos puede alcanzar el corto o mediano plazo y el momento en que ocurren es importante debido a que pueden existir compromisos relacionado con fechas límite.

3.7.2. Riesgos en cumplimientos de licenciamiento

- Actores: personal interno y externo.
- Tipo de amenaza: eventos malintencionados.
- Evento: ejecución inadecuada de control e instalación de software.
- Activo o recurso TI: procesos internos de TI.

- Riesgos: incumplimiento de los acuerdos de licenciamiento de software para el uso y distribución del mismo, sin la licencia respectiva o sobrepasando la cantidad de licencias autorizadas.
- Factores de impacto alto: la competencia, situación geográfica y política, el entorno regulatorio y legal del país, importancia estratégica de TI, capacidad de TI, capacidad para administrar TI, la complejidad del negocio y la capacidad para administrar los riesgos.
- Factores de impacto medio: el entorno tecnológico que cambia constantemente y capacidad de cambio del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección va del corto al mediano plazo.

3.7.3. Riesgos en cumplimientos de regulaciones

- Actores: personal interno y externo.
- Tipo de amenaza: eventos malintencionados.
- Evento: ejecución inadecuada.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: incumplimiento de los acuerdos adquiridos debido a la naturaleza del negocio, omisión de regulaciones de acuerdos con aseguradoras u otras organizaciones del sector público o del sector privado.
- Factores de impacto alto: la situación económica, entorno regulatorio y legal del país, importancia estratégica de TI, capacidad de TI, capacidad para administrar TI, la complejidad del negocio, la capacidad de cambio del negocio y la capacidad para administrar los riesgos.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto o mediano plazo. El momento en que ocurren los eventos es importante debido a que puede existir compromisos con fechas límite.

3.8. Riesgos en cumplimiento legal en Guatemala

3.8.1. Riesgos en cumplimiento legal en Guatemala

- Actores: personal interno.
- Tipo de amenaza: eventos malintencionados.
- Evento: ejecución inadecuada.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: incumplimiento de los decretos y acuerdos establecidos en el marco legal del país.
- Factores de impacto alto: la situación geográfica y política, el entorno regulatorio y legal del país, la importancia estratégica de TI, capacidad de TI, capacidad para administrar TI y para administrar los riesgos.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto o mediano plazo. El momento en que ocurren los eventos es importante debido a que puede existir regulaciones que impongan fechas límite.

En Guatemala al igual que otros países, existen leyes que regulan a nivel país aspectos relacionados con TI.

Es importante para las organizaciones conocer los aspectos legales que las regulan para evitar incumplimientos. Por ejemplo, se presentan algunas de las leyes vigentes en el país actualmente y que se han publicado en el sitio Web del Congreso de Guatemala:

- Decretos 33-98 y 56-2000 del Congreso de la República de Guatemala, que describen los derechos de autor y derechos conexos. En esta ley se hace referencia a los derechos de autor; se describe cómo se definen los derechos de autor para los programas de ordenador, menciona aspectos relacionados a las copias ilícitas o no autorizadas, etc.

- Decreto 57-2000 del Congreso de la República de Guatemala, que constituye la ley de Propiedad Industrial. Esta ley tiene como uno de sus objetivos la protección a la creatividad intelectual, que tenga aplicación en el campo de la industria y el comercio.

- Acuerdo de la Superintendencia de Administración Tributaria 24-2007, el cual establece el régimen optativo de la factura electrónica FACE. Este acuerdo describe aspectos sobre la autorización, transmisión, conservación, almacenamiento y control de las facturas, notas de crédito y débito por medios electrónicos, así como su debido resguardo.

- Decreto 47-2008 del Congreso de la República de Guatemala, que constituye la ley para el reconocimiento de las comunicaciones y firmas electrónicas.

- Decreto 57-2008 del Congreso de la República de Guatemala, que regula el acceso a la información pública y que tiene como objetivo garantizar el derecho a todas las personas que tengan interés a solicitar y obtener el acceso a la información pública que esté en posesión de las autoridades.

3.9. Otros escenarios de riesgos

3.9.1. Riesgos en la rendición de cuentas de TI

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: ejecución inadecuada.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: el negocio puede dejar de tomar su lugar de responsabilidad sobre el involucramiento en las áreas de TI y desaprovechar los recursos disponibles.
- Factores de impacto alto: el entorno regulatorio y legal del país, la importancia estratégica de TI, capacidad de TI, capacidad para administrar TI, complejidad del negocio, y la capacidad para administrar los riesgos.
- Factores de impacto medio: la competencia.
- Factor tiempo: el tiempo de duración puede ser amplio.

3.9.2. Riesgos de integrar TI en los procesos de negocio

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: estrategia inadecuada para la integración del negocio con TI.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: los procesos de negocio y las soluciones no están integradas.
- Riesgo positivo u oportunidad: la integración de las operaciones y las soluciones de TI optimiza los recursos empresariales incluyendo a las personas.

- Factores de impacto alto: la situación económica, el entorno regulatorio y legal del país, la competencia, la importancia estratégica de TI, capacidad de TI, capacidad para administrar TI, la complejidad del negocio, capacidad de cambio del negocio y la capacidad para administrar los riesgos.
- Factores de impacto medio: la situación geográfica y política.
- Factor tiempo: el tiempo que dura el efecto del riesgo puede ir del mediano al largo plazo.

3.9.3. Riesgos en errores operativos de TI

- Actores: personal interno.
- Tipo de amenaza: eventos malintencionados y accidentales.
- Evento: ejecución inadecuada y cambios inadecuados.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: errores al momento de estar ejecutando procesos operativos de TI. Por ejemplo, durante el mantenimiento de sistemas, durante la ejecución de procesos de *backup*, etc.
- Factores de impacto alto: la importancia estratégica de TI, la capacidad de TI, la capacidad para administrar TI y para administrar los riesgos.
- Factores de impacto medio: la complejidad del negocio y la capacidad de cambio del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto o mediano plazo. El momento en que ocurren los eventos es importante debido a que pueden afectar las operaciones del negocio por un periodo de tiempo crítico.

3.9.4. Riesgos en procesos operativos de TI

- Actores: personal interno.
- Tipo de amenaza: falla.
- Evento: diseño y ejecución inadecuada del plan de operaciones de TI.
- Activo o recurso TI: procesos internos de TI.
- Riesgos: un diseño inadecuado o inexistente del plan de operaciones de TI puede inducir a fallas en la continuidad de los servicios y provocar errores permanentemente en la ejecución de procesos.
- Factores de impacto alto: la importancia estratégica de TI, capacidad de TI, capacidad para administrar TI y para administrar los riesgos.
- Factores de impacto medio: la complejidad del negocio y la capacidad de cambio del negocio.
- Factor tiempo: el tiempo que transcurre entre el evento y su detección es corto plazo. El momento en que ocurren los eventos es importante, debido a que pueden afectar las operaciones del negocio por un período de tiempo crítico. La duración de las interrupciones del servicio pueden ser cortas o de mediano plazo.

4. GESTIÓN DE RIESGOS EN GUATEMALA

4.1. Investigación sobre gestión de riesgos en el medio

Debido al avance que la tecnología de la información ha tenido en los últimos años, incluso en nuestro medio, su uso se ha incrementado y las empresas u organizaciones se apoyan en ella para la realización de sus operaciones. Sin embargo, surge la inquietud sobre cómo las empresas en el medio guatemalteco están enfrentando el reto que representa la adecuada gestión del riesgo corporativo de TI.

En Guatemala por medio del Registro Mercantil, entidad del Estado, se han inscrito empresas de diferentes tipos, tales como: sociedades nacionales, extranjeras y empresas mercantiles.

Las empresas pueden manejar de diferentes maneras los servicios y recursos de TI. Por ejemplo, subcontratar los servicios con proveedores, comprar productos adquiriendo contratos de mantenimiento y administrar los servicios y recursos de TI con personal interno. Las empresas pequeñas, incluso operan sin un departamento de informática que les provea servicios y únicamente se adquieren los recursos básicos como equipos, servicio de internet y aplicaciones de oficina.

Por otro lado, existe el conjunto de personas que trabajan activamente en los departamentos de informática de las empresas u organizaciones ya sean proveedoras de servicios para una o más empresas o empleados de departamentos de informática pertenecientes a la estructura organizacional.

Ante esta realidad se decidió elaborar una encuesta destinada a personas que han tenido la experiencia de trabajar dentro de cualquier área de informática y quienes conocen cómo se realizan las actividades internamente; además, que han experimentado consciente o inconscientemente en su actividad laboral los escenarios de riesgos descritos con anterioridad y conocen si existen los controles necesarios que apoyen su respectiva gestión.

Los resultados de la encuesta permitirán responder a preguntas sobre el estado actual de la gestión de los riesgos relacionados con TI, en el medio corporativo guatemalteco.

La encuesta fue publicada en internet en la dirección siguiente: https://spreadsheets.google.com/viewform?formkey=dHFpVXl1Y3JQNk9pSkxud0NFSW1mdVE6MQ.

Adicionalmente, se realizaron impresiones de la encuesta, las cuales fueron distribuidas directamente a personas con el perfil requerido en diferentes lugares, incluyendo a personas que se encontraban en el interior del país. Posteriormente, fueron ingresadas en internet para unificar las respuestas.

Se definieron 10 preguntas y fueron respondidas por 337 personas que se desempeñan dentro de las áreas de TI. Se estima que la cantidad de encuestados es aceptable, tomando como base la fórmula para estimar una proporción sobre una población infinita.

La base para no utilizar la fórmula finita es por los motivos siguientes: primero, en el sitio Web del Registro Mercantil de Guatemala, está disponible la estadística de empresas inscritas desde el 2000, sin embargo, no abarca la totalidad. Segundo, no todas las empresas inscritas tienen un centro de informática, especialmente las pequeñas empresas y tercero las que sí lo tienen, en algunos casos, es compartida por otras empresas; por ejemplo, casos como corporaciones que tienen inscritas varias empresas.

A continuación se describe la fórmula:

$$n = Z_{\alpha}^{2} \frac{\mathrm{p} \,.\, (1 - \mathrm{p})}{\mathrm{i}^{2}}$$

En la fórmula anterior, cada una de sus variables significa lo siguiente:

- n: es el tamaño de la muestra
- Z: representa el nivel de confianza
- p: prevalencia o proporción esperada
- i: describe el error que se prevé cometer

Los valores que se asignaron para calcular el tamaño de la muestra son los siguientes:

- Z: 1.96 para un nivel de confianza del 95 %. Donde α = 0.05, de (1-0.95).
- p = 0.04
- i = 0.0525

$$n = 1.96^2 \ \frac{0.4(1-0.4)}{0.0525^2}$$

$$n = \frac{0.92198}{0.00276}$$

$$n = 334.05 \ \approx \ 334$$

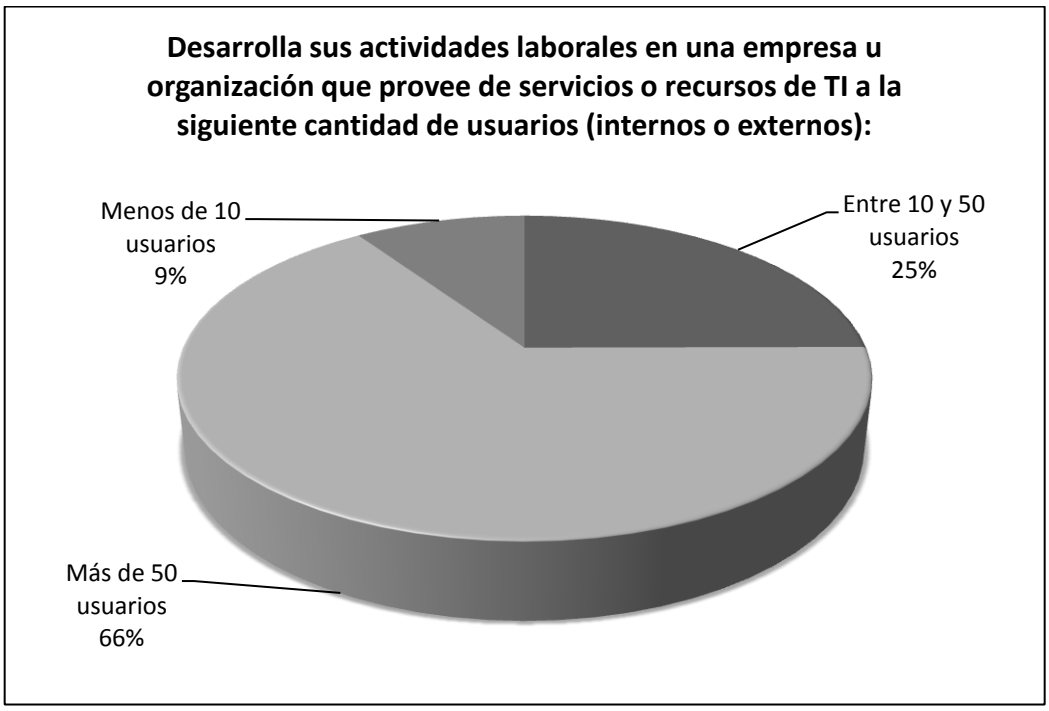
De acuerdo con este resultado, el tamaño mínimo de la muestra es de 334 encuestas.

4.1.1. Resultados de la encuesta

El análisis que se va a presentar inicia con la obtención de la información de la cantidad de usuarios que son atendidos por TI donde el encuestado labora. ¿Cuántos usuarios son atendidos?, es una pregunta que busca determinar la cantidad de personas que hacen uso o reciben algún servicio de TI y es probable que sea diferente al número de colaboradores que trabajan en una entidad.

La figura 4, presenta el parámetro de comparación sobre la utilización y posible dependencia que tiene el negocio de TI.

Figura 4. **Número de usuarios que son atendidos**



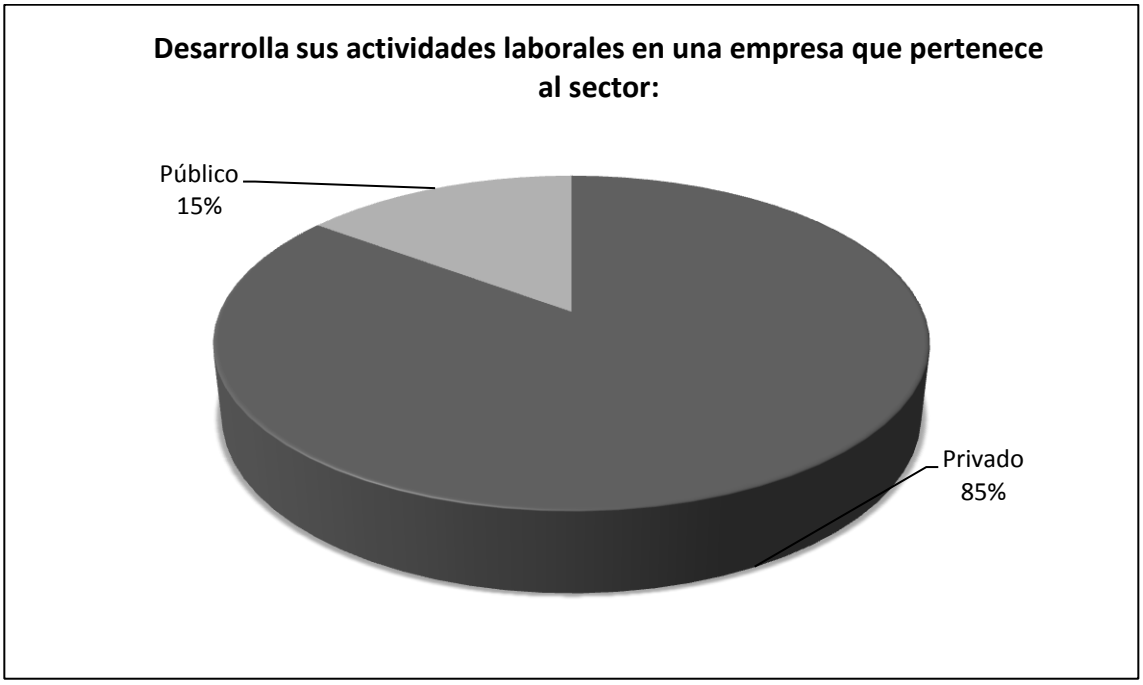
Fuente: elaboración propia.

Uno de los factores para determinar la importancia y grado de complejidad de TI es debido a la cantidad de usuarios; las respuestas recibidas corresponden a aquellas que tienen mayor porcentaje de servicio.

Además, la participación del resto es significativa y permite dar una vista completa del estado actual del medio empresarial.

Adicionalmente, la muestra fue seleccionada para tener representatividad de los sectores público y privado del país. La figura 5 a continuación, presenta esta información:

Figura 5. **Sector al que pertenece la empresa u organización**



Fuente: elaboración propia.

Los resultados que se obtuvieron tienen una composición representativa en el entorno empresarial nacional, debido a que la cantidad de empresas en el sector privado es muy superior al número de organizaciones en el sector público del país.

¿Será importante la gestión de riesgos para las organizaciones? En la Figura 6 que se presenta a continuación se describen los resultados que demuestran que en las empresas han designado a alguna persona responsable de administrar los riesgos corporativos.

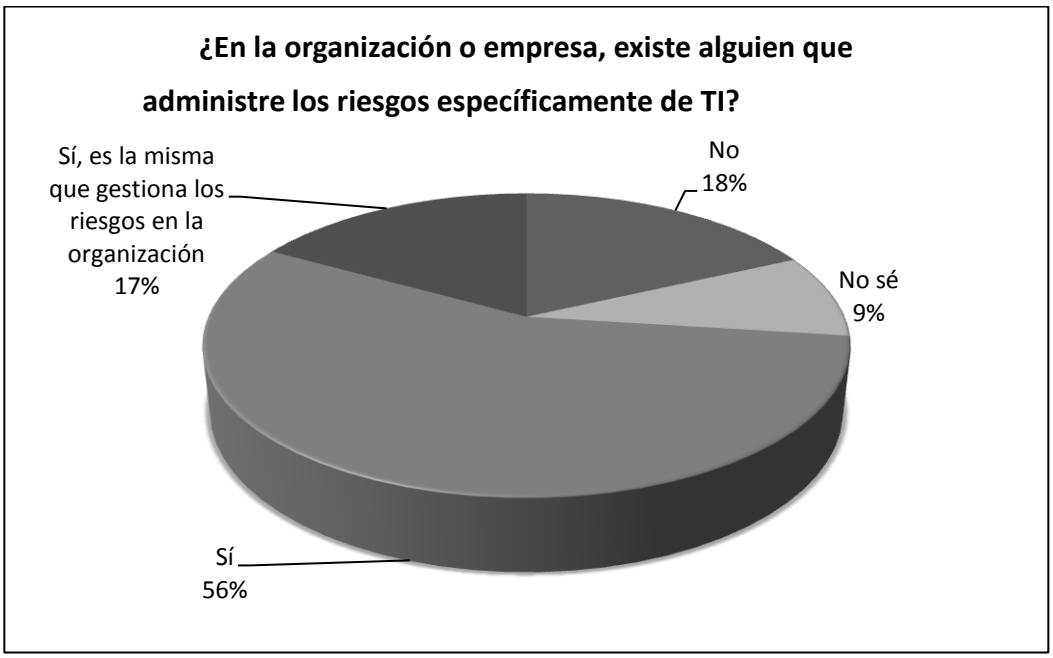
Figura 6. **Administrador de riesgos en la organización**

Fuente: elaboración propia.

Los valores indican que en el medio corporativo empresarial en Guatemala, es importante la gestión de los riesgos y existe una persona con la responsabilidad de administrarlos. Esta respuesta nos da la orientación acerca de la estrategia de administración de las empresas; sin embargo, es sólo un elemento que debe ser completado por el despliegue de las actividades que esto implica.

El aspecto que realza este estudio se refiere a conocer cómo los riesgos de TI son gestionados. Se desea conocer si existe alguien que se encargue de la gestión de riesgos de TI en la organización. La figura 7 responde a esta inquietud.

Figura 7. **Administrador de riesgos de TI en la organización**



Fuente: elaboración propia.

Es interesante notar que la proporción se mantiene en las organizaciones ante el hecho de tener un responsable de la administración de riesgos de TI y a su vez tener a alguien que gestione los riesgos a nivel corporativo, aunque en algunos casos sea la misma persona.

Las últimas dos interrogantes nos dan un punto de partida, de que existe interés en las organizaciones para manejar los riesgos apropiadamente y que han asignado responsables para facilitar la realización de actividades relacionadas con la gestión.

Con dos objetivos propuestos, se ha planteado la consulta acerca del inventario, portafolio o perfil de riesgos de TI. ¿Es un término que sea conocido

o previamente escuchado en el ámbito de trabajo del encuestado? La figura 8 a continuación nos da la información para realizar el análisis correspondiente.

Figura 8. **Portafolio o perfil de riesgos de TI**

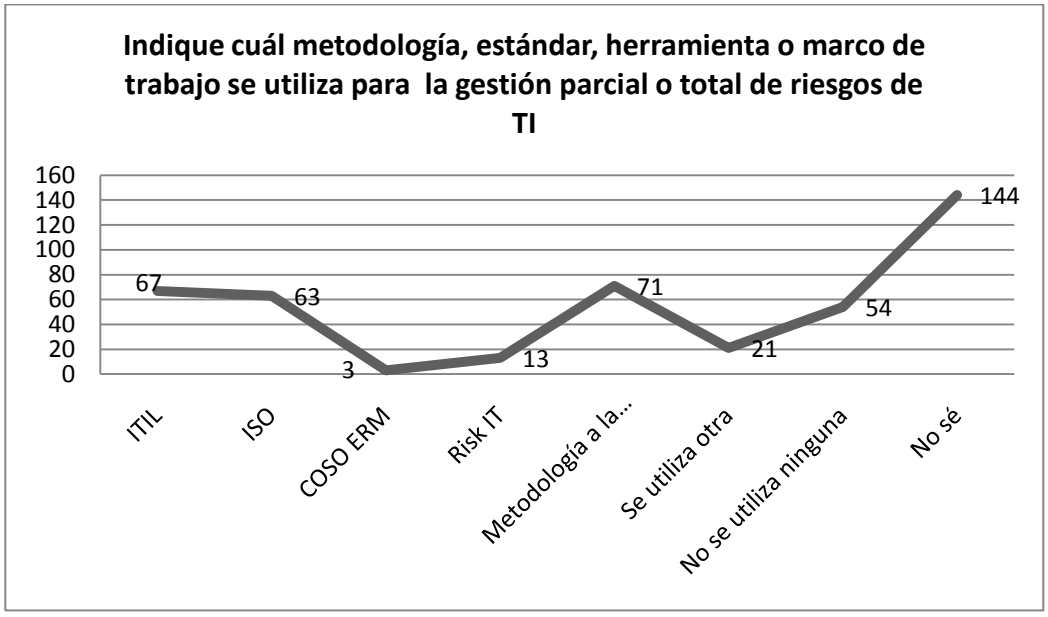
Fuente: elaboración propia.

Para las organizaciones, el disponer de un inventario de riesgos representa tener una visión completa de los riesgos a los que se deben enfrentar, es muy alentador conocer que una cantidad importante de ellas lo tienen y lo han comunicado. Por otro lado, en la mayoría de organizaciones, a pesar de contar con personas responsables, no se dispone del portafolio; teniendo en el mejor de los casos sólo el alcance parcial de solución.

También se hizo la consulta sobre ¿cuál es la metodología, estándar, herramienta o marco de trabajo que se utiliza para la administración de riesgos de TI?

La figura 9 presenta los resultados obtenidos y se ha identificado que existe una tendencia hacia el uso de ITIL, estándares ISO y metodologías propias.

Figura 9. **¿Qué se utiliza para la gestión de riesgos de TI?**

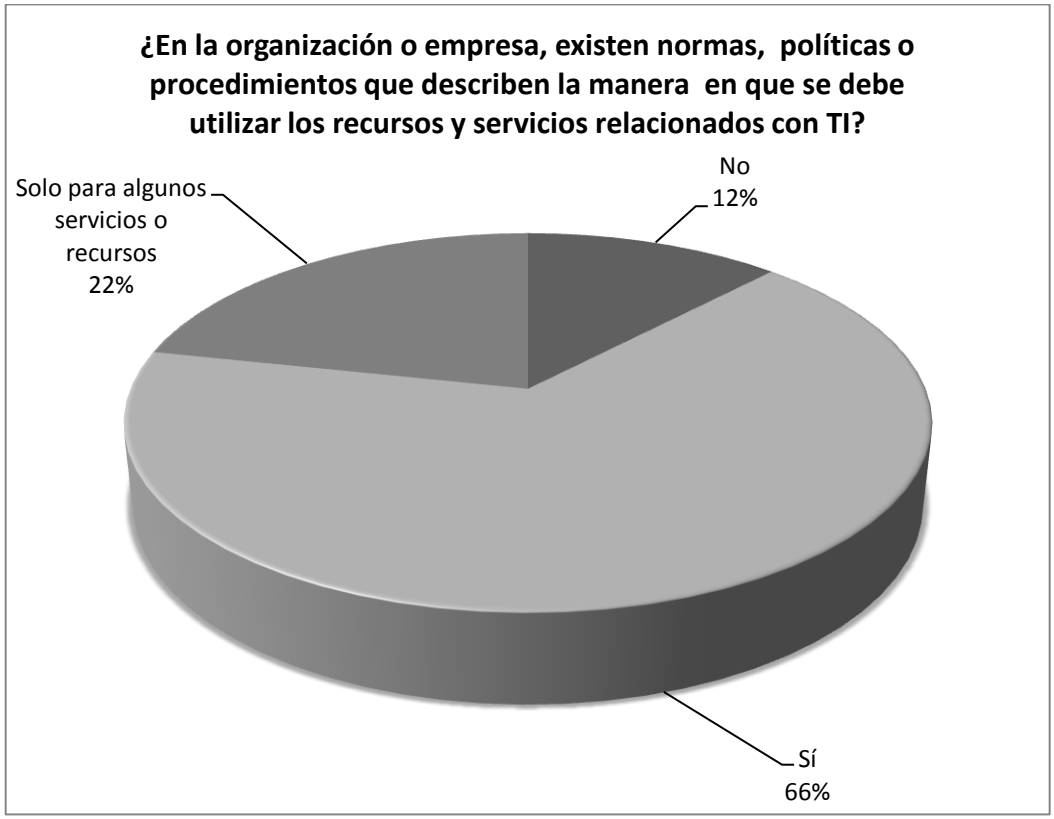


Fuente: elaboración propia.

En esta pregunta se permitió elegir más de una opción de respuesta por encuesta. Esto representa que en algunas organizaciones se tiene más de una manera de gestionar los riesgos de TI. Por el contrario, se debe tener precaución respecto de que en la mayoría de casos, no se realizan acciones o no se tenía la información necesaria para responder la pregunta. Esto podría deberse a la falta de comunicación interna o bien, que los procedimientos y controles internos de TI ya se encuentren definidos con anterioridad y las personas no estén familiarizadas con los nombres técnicos correspondientes.

Continuando con el análisis, ahora se verá si se han tomado acciones para regular el uso de los recursos y servicios de TI.

Figura 10. **Acciones para regular y controlar los recursos y servicios de TI**

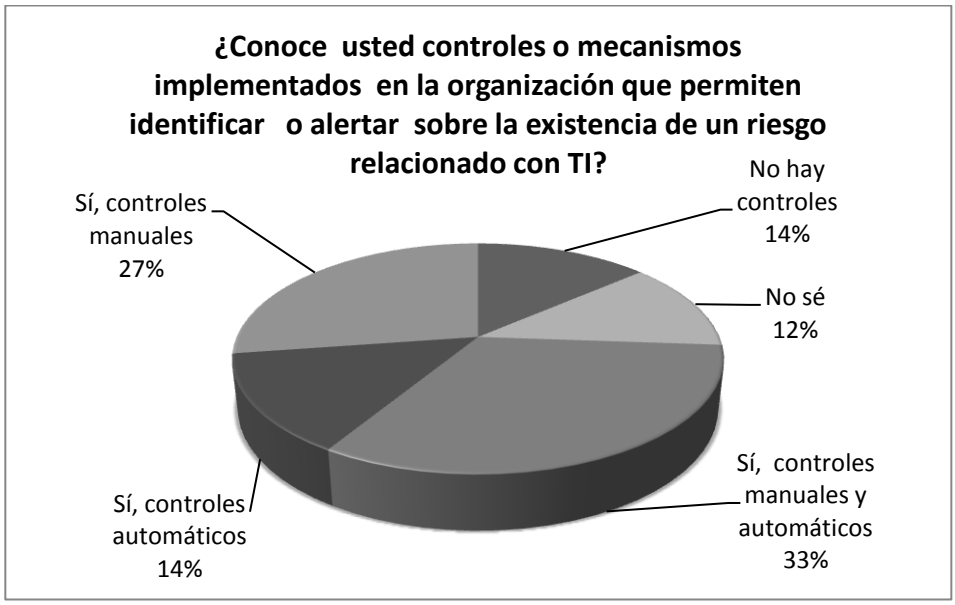


Fuente: elaboración propia.

Se considera que la mayoría de organizaciones o empresas tienen lineamientos definidos que les permite una adecuada administración de los recursos y servicios de TI. Existe una oportunidad de mejora para aquellos casos donde no se tiene ningún lineamiento o solamente se tiene para algunos servicios o recursos.

Aún cuando una empresa tenga lineamientos definidos, es importante conocer si se puede asegurar su cumplimiento. Para ello, se hizo la consulta acerca de los mecanismos que la persona conozca que alerten ante la existencia de un riesgo en sus áreas de trabajo.

Figura 11. **Mecanismos de control**

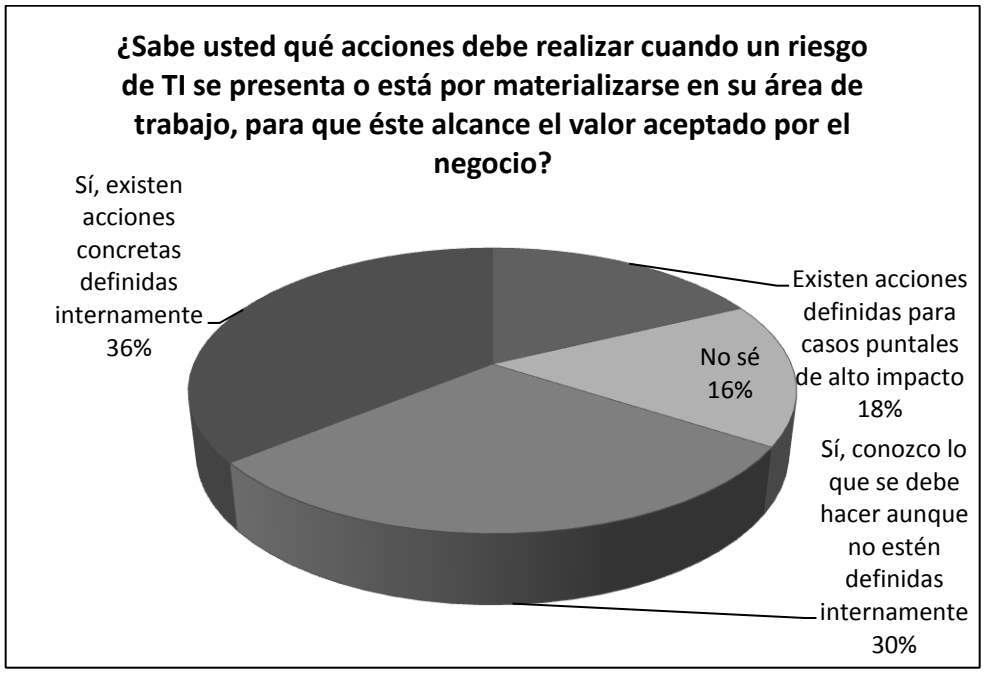


Fuente: elaboración propia.

En el medio guatemalteco, donde se ha realizado el estudio, se observa diversidad de escenarios que van desde no tener controles hasta tenerlos de forma automatizada. Esta pregunta revela el nivel de madurez que las organizaciones poseen, porque al tener un nivel alto, los mecanismos de control para responder a los riesgos tienen una tendencia a la automatización. Aunque también se reconoce que un grupo importante está haciendo esfuerzos manuales que apoyen la gestión del riesgo. De nuevo la oportunidad de mejora se presenta para todos los casos que no tienen ningún control.

¿Cómo responden las empresas u organizaciones al riesgo? Si se ha detectado de forma manual o automática que se ha materializado un riesgo o esté próximo a presentarse, la acción de respuesta es trascendental para llevarlo hacia el valor que el negocio esté dispuesto a aceptar. La figura 12, a continuación, describe el conocimiento que se tiene en las empresas para responder al riesgo.

Figura 12. **Respuesta al riesgo**



Fuente: elaboración propia.

Se ha realizado un trabajo importante en el medio para poder responder a los riesgos, debido a que existe la definición sobre qué acciones se deben realizar. También se ve la necesidad de implementar cambios para formalizar las acciones de respuesta considerando el hecho de que las personas conocen lo que se debe hacer cuando los eventos del escenario de riesgo se presentan.

Por último, existió el interés de conocer la tendencia de la estrategia de TI en las organizaciones.

Figura 13. **Estrategia de TI en la organización**

Fuente: elaboración propia.

En una nación que está en vías de desarrollo, es positivo conocer que se tiene el interés organizacional de aprovechar la tecnología para crear productos, servicios y nuevas oportunidades de negocio.

También es importante reconocer que para alcanzar este objetivo estratégico y cumplirlo consistentemente, se hace necesario tener una base sólida de gestión de TI, que incluye necesariamente la administración de riesgos corporativos.

5. MARCO DE TRABAJO PARA LA GESTIÓN RIESGOS DE TI

El momento es oportuno para hacer un planteamiento que describa los pasos a seguir para la implementación de la gestión de riesgos en una organización, dónde iniciar, qué elementos se deben considerar, qué acciones se deben realizar y qué resultados serán obtenidos.

En este contexto es necesario tomar en cuenta tres elementos: primero, tener claro los objetivos organizacionales incluyendo los que tengan relación con la gestión de riesgos; segundo, conocer cuál es la complejidad propia de TI y tercero, determinar los niveles de madurez del estado actual y del que se desea alcanzar.

Con esta información se puede proponer la implementación del cambio del nivel de madurez de riesgos en la organización. Esto se facilita al considerar la diversidad de opciones entre marcos de trabajo, estándares y normas aplicables en la organización pese a sus características especiales. No obstante, su enfoque conceptual y metodológico, también tiene un sentido práctico.

Para que se alcance este objetivo, es fundamental que sea impulsado por las personas con autoridad en la estructura organizacional, como directores o gerentes.

Es preciso aclarar, que la administración de riesgos es un proceso que involucrará una mejora continua y que no termina con la implementación del mismo.

5.1. Marcos de trabajo, normas y estándares

La gestión de riesgos corporativos de TI abarca muchos aspectos en diferentes áreas de TI. Desde hace algunos años se han creado marcos de trabajo, metodologías y estándares destinados a administrar los riesgos.

A continuación se presentarán las características principales de algunos de los estándares, marcos de trabajo y modelos, con el objetivo de orientar acerca de cuál de ellos puede aplicarse, en qué circunstancias y tener la base que sustente una decisión presente o futura.

5.1.1. Marco de trabajo COSO ERM

Este marco de trabajo define los componentes necesarios para la gestión de riesgos empresariales. Se basa en principios y conceptos, fomenta un lenguaje común de riesgo organizacional a la vez que proporciona las directrices y orientación para su administración. Según el resumen ejecutivo COSO ERM, algunas de sus características son:

- Se enfoca en el cumplimiento de los objetivos de negocio.
- Minimiza las sorpresas y pérdidas operativas.
- Identifica y gestiona los riesgos para toda la organización.
- Fomenta ser proactivo y aprovechar las oportunidades generadas.
- Requiere establecer directrices descendentemente desde la parte superior organizacional hasta los niveles del personal operativo.
- El marco de trabajo está disponible al público por medio de pago.

5.1.2. Estándar ISO/IEC 27005:2011

Este estándar provee directrices para la gestión en los riesgos de seguridad de la información, requiere conocimientos previos de los estándares ISO/IEC 27001 e ISO/IEC 27002 quienes proveen información sobre conceptos, modelos, procesos y terminología utilizados. Se aplica en cualquier tipo de empresa u organización. Algunas de sus características son:

- Enfoque en la gestión de riegos relacionados con la seguridad de la información.
- Se alinea con los objetivos de negocio relacionados con la protección de la información.
- Provee un modelo de proceso detallado.
- Requiere establecer directrices descendentemente desde la parte superior en la estructura organizacional hasta el personal operativo.
- El estándar está disponible al público por medio de pago.

5.1.3. Estándar ISO/DIS 31000:2009

Este estándar provee principios y directrices de carácter genérico para la gestión de riesgo. Se aplica en cualquier tipo de empresa u organización porque no está creada sobre alguna industria o sector en particular. Algunas de sus características adicionales son:

- Se alinea con los objetivos de negocio.
- Permite su aplicación a lo largo de la vida de una organización.
- Es aplicable a cualquier tipo de riesgo, sin diferenciar su naturaleza, así como si tiene efecto positivo o negativo para la organización.

- Requiere establecer directrices descendentemente desde la parte superior en la estructura organizacional hasta el personal operativo.
- Provee un modelo de proceso detallado.
- El estándar está disponible al público por medio de pago.

5.1.4. Estándar AS/NZS 4360:2004

Este estándar tiene origen en Australia y Nueva Zelanda. Provee principios y directrices de carácter genérico para la gestión de riesgo corporativo. Se aplica en cualquier tipo de empresa u organización. Está basado en un conjunto de etapas que inician con el establecimiento del contexto del riesgo, con base en ello, se continúa con la identificación, análisis, evaluación y tratamiento de riesgos.

Algunas de sus características adicionales son:

- Se alinea con los objetivos de negocio.
- Requiere establecer directrices descendentemente desde la parte superior en la estructura organizacional hasta el personal operativo.
- Provee un modelo de proceso detallado.
- El estándar está disponible al público por medio de pago.
- Identifica y gestiona los riesgos para toda la organización.

5.1.5. Marco de trabajo Risk IT

Risk IT, es un marco de trabajo con enfoque práctico que tiene como base un conjunto de principios para guiar la gestión integral de los riesgos de TI. Algunas de sus características son:

- Se alinea con los objetivos de negocio.
- Promueve la integración de los riesgos de TI con los riesgos de toda la organización.
- Posee una vista integral sobre todos los riesgos de TI. Incluye ejemplos prácticos.
- Requiere establecer directrices descendentemente desde la parte superior organizacional hasta los niveles del personal operativo.
- Se encuentra disponible para el público en general.
- Provee un modelo de proceso detallado e incluye instrucciones para casos de riesgo específicos.

5.1.6. PMBOK IEEE Estándar 1490-2003

Estándar que proporciona directrices, reglas y principios para la gestión de proyectos y su debida gestión de riesgos. Algunas de sus características son:

- Se alinea con los objetivos de negocio.
- Vista parcial sobre riesgos de TI en el área de administración de proyectos.
- Requiere establecer directrices descendentemente desde la parte superior organizacional hasta los niveles del personal operativo.
- Provee un modelo de proceso detallado.

- El estándar está disponible al público por medio de pago.

5.1.7. MAGERIT

Es una metodología para el análisis y gestión de riesgos. Fue creado por el Ministerio español de Administraciones Públicas. Algunas de sus características son:

- Mantiene la unión con los objetivos de negocio aunque solo parcialmente debido a su enfoque muy particular.
- Su perspectiva son los riesgos de sistemas de información de TI y su entorno.
- Se encuentra disponible para el público en general.
- Provee un modelo de proceso detallado.

5.1.8. COBIT

Es un marco de trabajo creado por ISACA, cuyo enfoque está basado en las tecnologías de la información y el gobierno de TI. Tiene como objetivo la reducción de la brecha entre las necesidades de control, los aspectos técnicos y los riesgos del negocio. A su vez, promueve el establecimiento de políticas claras y propone un conjunto de buenas prácticas para las aéreas de TI. Algunas de sus características adicionales son:

- Se alinea con los objetivos de negocio.
- Requiere establecer directrices descendentemente desde la parte superior organizacional hasta los niveles del personal operativo.
- Provee un modelo de proceso detallado.
- Se complementa con Risk IT.

5.1.9. ITIL

Es un marco de trabajo creado por la oficina gubernativa de comercio del Reino Unido, cuyo enfoque reside en la gestión de servicios.

Provee un conjunto de mejores prácticas para identificar, planificar entregar y mantener los servicios de TI con el negocio. ITIL aborda los riesgos en varios procesos descritos en la versión dos y tres. Algunas de sus características son:

- Se alinea con los objetivos de negocio.
- Vista específica para el área de servicios TI.
- Requiere establecer directrices descendentemente desde la parte superior organizacional hasta los niveles del personal operativo.
- Provee un modelo de proceso detallado.

5.2. Establecer el nivel de madurez

Conviene ahora realizar un análisis objetivo y conocer cuál es la situación actual y futura en la organización respecto del nivel de madurez en la gestión de riesgos. Para ello puede apoyarse en las siguientes preguntas:

- ¿Las estrategias de TI se enfocan a alcanzar los objetivos del negocio?
- ¿Cuál es el nivel de complejidad de TI?
- ¿Cuál es el nivel de madurez que se pretende alcanzar?
- ¿Cuál es el nivel actual de madurez?

Para responder a estas interrogantes se hace necesario profundizar en los siguientes puntos:

5.2.1. Alineación de estrategia del negocio y objetivos de TI

El potencial en servicios y soluciones que TI puede ofrecer es amplio y se debe tener claro desde el inicio cuáles son los objetivos hacia los que se deben dirigir todas las acciones.

Para ello, se debe listar y comparar los objetivos del negocio con los objetivos de TI. Cualquier diferencia al respecto debe ser tratada a nivel estratégico. Por ejemplo, si una organización bancaria tiene establecido impulsar los servicios electrónicos y detener el crecimiento en el número de sus agencias, la estrategia de TI debe estar enfocada en habilitar los servicios requeridos bajo una plataforma tecnológica que le sustente de forma sostenible, asegurando que los riesgos relacionados estén administrados de forma eficaz.

Es probable que se deba reorganizar los recursos económicos, los recursos humanos, modificar la clasificación actual y futura de los proyectos, realizando ajustes en el grado de importancia y priorización asignada. Aunque exista la tendencia natural a pensar que es muy fácil de hacer, su realización podría requerir esfuerzos adicionales. Esto puede ocurrir, por ejemplo, si la estrategia de TI está enfocada en minimizar sus costos, mientras que la estrategia del negocio puede estar demandando más servicios y nuevos productos.

5.2.2. Evaluación de la complejidad de TI

El nivel de complejidad de TI proporcionará valiosa información para determinar el control necesario según las características propias de la organización.

Una organización que tenga un tamaño grande en infraestructura física o personal no significa necesariamente que tenga un área de TI con mucha complejidad o sofisticación. Lo mismo aplica en el sentido opuesto, pensando en una empresa que sea pequeña en tamaño físico o de personas, no significa necesariamente que su área de TI es simple. Entonces, ¿cuáles son aquellos elementos que ayuden a determinar la complejidad de TI?

De acuerdo con la revista ISACA Journal, a continuación se describen los aspectos que permiten medir el nivel o grado complejidad o sofisticación incluyendo los valores bajo, mediano o alto:

- Cantidad de servidores: grado bajo, si tiene cero o un servidor; medio, si tiene dos o tres servidores y alto si tiene tres o más.

- Cantidad de estaciones de trabajo: grado bajo, si tiene menos de 16; medio, si tiene entre 16 y 30, y alto, si la cantidad es mayor que 30.

- Aplicaciones: grado bajo, si tiene únicamente aplicaciones de oficina como Microsoft Office, Open Office, etc. y son utilizadas con las funcionalidades básicas. Grado medio, si tiene aplicaciones a la medida, o incluso aplicaciones de oficina aunque con uso avanzado. Además, si información importante de la organización se está procesando en estos programas.

Por último, grado alto, si poseen aplicaciones a la medida complejas o software comercial de uso corporativo, por ejemplo sistemas ERP.

- Ubicaciones remotas: grado bajo, si no se tiene ninguna ubicación remota; medio, si tiene hasta dos estaciones remotas y clasificación alta, si tiene más de dos.

- Transacciones en línea: clasificación baja, si carece de estas transacciones; grado medio, si tiene algunas operaciones en línea y alto, si tiene muchas operaciones en línea en un periodo corto de tiempo; por ejemplo, tener miles de operaciones en línea durante un día.

- Redes. Grado bajo, si no tiene conectividad de red; grado medio, si tiene una infraestructura de red dentro de una ubicación física, por ejemplo un edificio, y grado alto, si tiene redes en diferentes sedes y están interconectadas entre sí.

- Tecnologías de TI nuevas o avanzadas. Grado bajo, cuando el uso de tecnología nueva o avanzada no existe o solamente en poca medida; grado medio, cuando se utiliza en forma moderada, clasificación alta, al utilizar en forma moderada con tendencia a incrementar su uso.

5.2.3. Determinar el nivel de madurez

El siguiente paso consiste en asignar el nivel de madurez que se desea alcanzar de acuerdo con los objetivos de negocio y además estimar el estado actual. Los niveles de madurez explicados a inicios de este estudio son 6 y van del nivel 0 al 5.

Al resumirlos brevemente, se tiene que en el nivel 0 no existe gestión de riesgos y ninguna acción se realiza; el nivel 1 o el inicial se determina cuando se carece de orden en la gestión; el nivel 2 o repetible, ocurre cuando se aborda el riesgo de una forma regular y se dan muestras de orden y estandarización; en el nivel 3 o definido, ya se alcanza cuando existe madurez en los procesos de documentación y comunicación como resultado de la gestión; el nivel 4 gestionado, significa que existen mediciones y son supervisadas. Por último, el nivel 5 u optimizado, es aquel en el que las mejores prácticas son implementadas y automatizadas.

Es conveniente aclarar que en algunas áreas o procesos puede existir diferencia entre el nivel de madurez. Por ejemplo, en lo que respecta a la gestión de servicios puede tener un nivel 4 donde ya se tengan métricas que son supervisadas continuamente y por otro lado en otra área donde se gestionan los proyectos de TI y en esa parte se tenga un nivel de madurez 2, considerando que la gestión de riesgos de basa solamente en la intuición de los expertos.

La importancia de esta actividad consiste en ubicar dentro de la organización el estado actual y futuro del nivel de madurez, incluso aunque se decida hacerlo por áreas, iniciando por las que tengan mayor impacto sobre los objetivos organizacionales.

5.2.4. Impulsar el cambio desde el nivel de dirección

Hasta este momento se ha reunido la información mínima necesaria para implementar el cambio en el nivel de madurez referente a la administración de riesgos en la organización.

Para lograrlo será necesario iniciar, incrementar o perfeccionar el uso o realización de más de uno de los siguientes aspectos:

- La comunicación
- Implementar controles por medio de políticas, normas y procedimientos
- La responsabilidad, compromiso, supervisión y rendición de cuentas
- Uso de las herramientas, metodologías, marcos de trabajo o estándares
- Uso de la tecnología para automatizar las tareas

Para dar forma a la solución, las personas con poder de toma de decisiones deben analizar en conjunto los objetivos del negocio, la complejidad de TI, los niveles de madurez de riesgos presentes y deseados en la organización, para determinar el camino que se debe seguir.

5.3. Implementación de gestión de riesgos enfoque práctico

La gestión de riesgos no es solo un proyecto que se realiza una vez, por el contrario, constituye un proceso que involucrará una mejora continua y con el objetivo de poner la base para su implementación, los pasos propuestos se describen a continuación:

5.3.1. Obtener directrices del nivel ejecutivo

El nivel ejecutivo, los directores y gerentes a cargo del gobierno de la organización, deberán realizar las siguientes acciones:

- Definir el alcance de la gestión de riesgos de TI promoviendo los objetivos estratégicos que le sustenten dentro de la organización. Para ello dispondrán de la información acerca de la complejidad de TI y el estado actual del nivel de madurez. Además, deben considerar la complejidad, situación económica y los recursos disponibles en el negocio. Por ejemplo, definir el objetivo de gestionar los riesgos relacionados con la administración de proyectos, para apoyar el cumplimiento del objetivo estratégico que indica qué TI deberá ser generadora de valor en la organización y facilitar la activación de un servicio innovador cada trimestre.

- Determinar los valores que se tomarán como aceptables del riesgo. Estos límites son importantes, porque cuando se evalúe el costo en términos de dinero, recursos físicos, tiempo y personas que se necesitan para la implementación de la respuesta a los riesgos, el mismo no debe exceder al valor aceptado. Por ejemplo, en la gestión de proyectos el límite de variación para el tiempo entrega de proyectos es de 3 % del tiempo total, siempre y cuando tenga una justificación válida.

- Decidir integrar los riesgos de TI con los riesgos empresariales. Esto permitirá tener una vista global de riesgos en toda la organización. La persona que gestiona los riesgos de las áreas de negocio, puede ser la misma que se encargue de la gestión de los riesgos de TI, solamente debe estar asesorada por personal técnico calificado. De otra manera, si

se designa una persona de TI para la gestión de sus riesgos deberá rendir cuentas e informes al encargado a nivel organización.

5.3.2. Evaluación de los riesgos

La evaluación de los riesgos es una etapa que involucra las actividades relacionadas con la obtención de la información, análisis y elaboración del portafolio de riesgos de TI, que puede ser adherido al portafolio de la organización, según lo presentado en el capítulo 2.

Este estudio se basa en un listado genérico de escenario de riesgos que son comunes para las organizaciones. No obstante, se debe complementar utilizando técnicas que facilitan la colección de información, tales como entrevistas, lluvias de ideas, encuestas, observación, análisis de eventos históricos en el contexto organizacional, etcétera.

Como resultado de la evaluación de riesgos se debe obtener el portafolio o perfil de riesgos de TI.

En el capítulo tercero, como parte de este estudio, se han coleccionado los escenarios de riesgos de TI, donde se presenta para cada uno de ellos, la información para el análisis correspondiente, que incluye: los actores, el tipo de amenaza, el evento o eventos relacionados, los activos o recursos, los riesgos, los factores que tienen un impacto alto y la descripción de la influencia del factor tiempo. A continuación se presenta el listado de los escenarios de riesgos:

Tabla II. **Matriz de trabajo de escenarios de riesgo**

Ámbito del escenario de riesgo	**Escenario de riesgo**
Infraestructura física de TI	Obsolescencia
	Daño o destrucción
	Robo
	Inadecuada arquitectura
	Instalación y cambios
Relacionados con el personal de TI	Ausencia del personal
	Falta de habilidades y experiencia del personal
	Insuficiencia de personal especializado
Gestión de proyectos	Proyectos no finalizados
	Riesgos económicos del proyecto
	Retraso en entrega de proyectos
	Baja calidad en los proyectos
	Falta de visión de programa de proyectos
Gestión de la seguridad	Ataque lógico a la seguridad
	Traspasar la seguridad
	Alteración de la integridad de la información
	Exposición de la información
Aplicaciones	Incorrectas decisiones de inversión en aplicaciones
	Envejecimiento de las aplicaciones de negocio
	Implementación inadecuada de las aplicaciones
	Inestabilidad de las aplicaciones
	Falta de capacidad de las aplicaciones
	Envejecimiento de las aplicaciones de infraestructura
	Aplicaciones intrusas
Entrega y soporte de servicios de TI	Entrega y soporte de servicios
	Rendimiento de los servicios
Cumplimiento corporativo	Cumplimiento de acuerdos y compromisos
	Cumplimiento de licenciamiento
	Cumplimiento de regulaciones
Cumplimiento legal en Guatemala	Cumplimiento legal en Guatemala
Otros escenarios	Rendición de cuentas de TI
	Integración de TI y los procesos de Negocio
	Errores operativos de TI
	Procesos operativos de TI

Fuente: *The Risk IT Practitioner Guide*

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx

5.3.3. Controles

Se ha visto el panorama general organizacional referente a los riesgos que pueden ocurrir en TI, con la intención de presentar soluciones que permitan responder a los mismos de la forma esperada; esto significa que se debe determinar las acciones que lleven a la obtención del riesgo residual.

La respuesta a los riesgos puede hacerse de diferentes maneras: Aceptándolos, transfiriéndolos, compartiéndolos, reduciéndolos, explotándolos, mejorándolos y evitándolos. Sin embargo, para gestionar la respuesta al riesgo cuando se comparten, reducen, explotan o mejoran, se hace por medio de controles.

Tales controles son implementados por medio de procedimientos, políticas y mejores prácticas que influyen en el impacto o frecuencia de los eventos hasta que se alcancen los valores aceptados por el negocio.

A continuación, con base en el marco de trabajo de riesgos de TI, de ISACA, se presentan los controles sugeridos para cada uno de los escenarios de riesgos listados con anterioridad:

5.3.3.1. Riesgos en la infraestructura de TI

- Obsolescencia:
  - Realizar la evaluación de las capacidades actuales.
  - Fomentar la estandarización tecnológica.
  - Establecer la dirección para la planificación tecnológica.
  - Establecer un plan de adquisición que incluya el corto, mediano y largo plazo.

- Realizar el mantenimiento de la infraestructura de forma periódica según las recomendaciones de los fabricantes.

- Daño o destrucción de la infraestructura de TI
  - Establecer medidas de seguridad para prevenir, detectar y mitigar los riesgos debido a robo, fuego, agua, humo, actos vandálicos, etcétera.
  - Definir los procedimientos de seguridad de acceso físico, que incluyan la clasificación de áreas restringidas y a todas las personas. Tales accesos deben ser autorizados, registrados y supervisados.
  - Administrar las instalaciones físicas. Se deben establecer las medidas de control para el cumplimiento de normas, leyes y reglamentos acerca de la seguridad, normas de salud, normas operativas.

- Robo a la infraestructura de TI
  - Establecer la política interna de TI que regule el comportamiento, describa los roles, responsabilidades y rutas para la rendición de cuentas de cada una de las personas.
  - Procedimientos del personal. Incluye la revisión del proceso de contratación, con mayor énfasis en plazas que son críticas o sensibles para la organización.
  - Protección de la infraestructura. Se deben implementar los mecanismos de control interno de hardware y software asegurando que se deje registro de las actividades realizadas y permitir su posterior revisión. Asignar responsables para los componentes de la infraestructura que sean sensibles y además su uso debe ser supervisado.

- Inadecuada arquitectura de la infraestructura de TI
    - Establecer la dirección para la planificación tecnológica.
    - Establecer un proceso bidireccional y recíproco que involucre la planificación estratégica del negocio y la planificación tecnológica de TI y sus capacidades.
    - Disponer de un comité o grupo de especialistas de arquitectura, que provea de lineamientos y el conocimiento sobre cómo puede implementarse con resultados sostenibles en el tiempo.

- Riesgos en instalación y cambios a la infraestructura de TI
    - Establecer un plan de mantenimiento para la infraestructura, que incluya administración de actualizaciones y correcciones.
    - Establecer un procedimiento de gestión de cambios a la infraestructura y asegurarse que cada modificación se haga acorde a tal procedimiento.

5.3.3.2. Riesgos con el personal de TI

- Ausencia del personal clave de TI
    - Crear y mantener un inventario de personal y sus habilidades.
    - Minimizar la dependencia de personas claves por medio de la documentación, el intercambio de conocimiento entre empleados y la política de que cada persona clave le debe corresponder otra que sea su respaldo o sustituto en caso se ausente por un periodo de tiempo importante.

- Riesgos relacionados con la falta de habilidades del personal de TI
    - Establecer o alinear el proceso de reclutamiento con los procedimientos y normas de la organización.

- Crear y mantener un inventario de personal y sus habilidades.
- Evaluar el desempeño de sus empleados, acorde a sus responsabilidades, logros definidos y alcanzados.
- Mantener una política de mejora continua de las habilidades y conocimiento de sus empleados para que se facilite el logro de los objetivos.
- Mantener actualizado el perfil de los puestos de trabajo de TI, las competencias y requisitos necesarios para desempeñar la función apropiadamente.
- Comprender la demanda actual y futura del recurso humano y conocer las habilidades que serán necesarias para alcanzar los objetivos y asegurar su disponibilidad, lo cual involucra no tener ni excedentes ni faltantes.

- Personal insuficiente en TI
  - Crear y mantener un inventario de personal y sus habilidades.
  - Mantener actualizado el perfil de los puestos de trabajo de TI, las competencias y requisitos necesarios para desempeñar la función apropiadamente.
  - Comprender la demanda actual y futura del recurso humano y conocer las habilidades que serán necesarias para alcanzar los objetivos y asegurar su disponibilidad, lo cual involucra no tener ni excedentes ni faltantes.

5.3.3.3. Riesgos en la gestión de proyectos de TI

En la gestión de riesgos de proyectos se comentará acerca del programa de proyectos y del portafolio de proyectos. El portafolio se conoce como la agrupación total de proyectos, usualmente organizados en programas. Un programa es un grupo de proyectos que tienen al menos un objetivo global que cumplir y que es común en todos.

- Proyectos no finalizados
  - Establecer un marco de trabajo para la gestión de proyectos, que tenga lineamientos y mejores prácticas.
  - Implementar un comité de IT que se encargue de priorizar los programas de inversión para que estén alineados con la estrategia de la organización.
  - Elaborar un conjunto de mediciones que permitan evaluar el cumplimiento de los objetivos.
  - Establecer la preparación de informes para realizar revisiones periódicas del portafolio y programa de proyectos, evaluando su rendimiento.

- Riesgos económicos del proyecto
  - Establecer el procedimiento que administre los costos, comparando oportunamente los valores presupuestados con los datos reales. Identificar desviaciones y su impacto en el sentido de aceptar los incrementos o aceptar el costo de oportunidad de no hacerlo.

- Establecer los procedimientos para realizar el presupuesto de TI, que incluya los costos operativos, de mantenimiento, inversión y las prioridades. El procedimiento debe describir la manera de hacer el presupuesto para programas de proyectos individuales. También deben existir los pasos que admitan el refinamiento y aprobación.
- Establecer métricas, reportar a los interesados y monitorear los resultados de los proyectos. Enfocarse en aspectos de cronograma, costo y calidad. Identificar las desviaciones y el impacto en los resultados. Las métricas por ejemplo pueden ser: % de desviación en días del cronograma, % en moneda local de la variación del costo del proyecto con el costo presupuestado, cantidad de defectos o errores encontrados durante las fases de calidad de un producto.
- Implementar un comité de IT que se encargue de priorizar los programas de inversión para que estén alineados con la estrategia de la organización.
- Establecer la preparación de informes para realizar revisiones periódicas del portafolio y programa de proyectos, evaluando su rendimiento.

- Retraso en entrega de proyectos
  - Establecer métricas, reportar a los interesados y monitorear los resultados de los proyectos. Enfocarse en aspectos de cronograma, costo y calidad. Identificar las desviaciones y el impacto en los resultados.
  - Establecer métricas que permitan medir el desempeño del recurso que está trabajando, con dos objetivos: primero, tener una base para futuras estimaciones de tiempos de entrega. Segundo, comparar con el promedio del mercado y evaluar si se necesita hacer algunos cambios, como entrenamiento, balancear cargas de trabajo, etcétera.

- Establecer la preparación de informes para realizar revisiones periódicas del portafolio y programa de proyectos, evaluando su rendimiento.
- Implementar un comité de IT que se encargue de priorizar los programas de inversión para que estén alineados con la estrategia de la organización.
- Implementar los controles relacionados con el personal de TI.

- Baja calidad en los proyectos
  - Establecer un marco de trabajo para la gestión de proyectos, que tenga lineamientos y mejores prácticas.
  - Implementar en el proyecto la fase de planificación de la calidad del mismo, que describa especialmente los aspectos esperados en la calidad y hacer énfasis en las acciones que se deben tomar para verificarlo. Este plan debe ser revisado y acordado por las partes interesadas e incluido en el plan del proyecto.
  - Disponer de un comité o grupo de especialistas, que provea de lineamientos y el conocimiento necesario para implementar la tecnología con resultados sostenibles en el tiempo.
  - Establecer el compromiso con los interesados. Se debe obtener el compromiso y participación de los actores involucrados en la definición y ejecución de las actividades del proyecto.
  - Fomentar la estandarización tecnológica. En proyectos de software, establecer el uso de normas estándar para todo su ciclo de vida. Estandarizar el desarrollo de software, el uso de nombres, interfaces de usuario, informes, componentes de bases de datos, diseñarlo para permitir el crecimiento de operaciones sin degradar la calidad, asegurar el cumplimiento de los requisitos, efectuar pruebas de cada componente de software y su integración.

- Asegurar que los dueños del proceso de negocio, personal de TI e interesados, evalúen y aprueben el resultado de las pruebas de acuerdo con el plan establecido.
- En el cierre del proyecto, evaluar si se han obtenido los resultados y beneficios previstos. Informar a cada uno de los patrocinadores, usuarios y equipo del proyecto del cierre del mismo; además, retirar el proyecto del portafolio de proyectos. Documentar las lecciones aprendidas. Si no se han alcanzado los resultados deseados, evaluar las acciones necesarias para lograrlo.

- Falta de visión de programa de proyectos
  - Establecer un marco de trabajo para la gestión de proyectos, que tenga lineamientos y mejores prácticas.
  - Establecer métricas, reportar a los interesados y monitorear los resultados de los proyectos. Enfocarse en aspectos de cronograma, costo y calidad. Identificar las desviaciones y el impacto en los resultados.
  - Implementar un comité de IT que se encargue de priorizar los programas de inversión para que estén alineados con la estrategia de la organización.
  - Diseñar e implementar acuerdos de servicio y su correspondiente medición para facilitar la mejora continua.
  - Elaborar un conjunto de mediciones que permitan evaluar el cumplimiento de los objetivos.
  - Establecer la preparación de informes para realizar revisiones periódicas del portafolio y programa de proyectos, evaluando su rendimiento.

5.3.3.4. Riesgos en la seguridad en TI

- Ataque lógico a la seguridad
  - Establecer la política interna de TI que regule el comportamiento, describa los roles, responsabilidades y rutas, para la rendición de cuentas de cada una de las personas.
  - Desarrollar y mantener un plan de continuidad. Debe incluir instrucciones claras para obtener la recuperación de todos los servicios críticos de TI, responsabilidades y procedimientos de comunicación.
  - Establecer pruebas periódicas a la seguridad, implementar mecanismos de vigilancia, monitoreo y reporte que ayuden a la detección de traspaso a la seguridad.
  - Establecer medidas para prevenir, detectar y corregir la intromisión de software malicioso. Planificar las actualizaciones de seguridad y mantener actualizado el antivirus corporativo.
  - Establecer procedimientos y normas para la seguridad de la red. Utilizar técnicas y procedimientos de seguridad para autorizar o denegar el acceso y el control del flujo de información desde y hacia la red corporativa. Por ejemplo: implementación de firewalls, dispositivos de seguridad, segmentar las redes, implementar mecanismos detección de intrusos, etcétera.
  - Definir e implementar el procedimiento para la seguridad de la información, que describa la recepción, almacenamiento y salida de datos y que a su vez cumpla con los requisitos de negocio de la organización.
  - Incentivar la figura de propietario de datos y dueño de sistemas de información a los responsables de la información en el negocio.

- Traspasar la seguridad
    - Asegurar que todos los usuarios sin excepción estén identificados de forma única e inequívoca. Asegurar que para acceder a los recursos se requiera la debida autenticación que además permita confirmar que los accesos están debidamente autorizados y otorgados.
    - Establecer el procedimiento para la administración de usuarios y sus accesos. Clarificar los procesos de autorización, altas, modificación y bajas de usuarios y sus permisos.
    - Mantener actualizada la matriz de perfil de puestos y funciones, con un perfil de accesos estándar que permita admitir, autorizar y documentar las excepciones. Además, identificar la combinación de funciones que impliquen riesgo operativo.
    - Establecer pruebas periódicas a la seguridad, implementar mecanismos de vigilancia, monitoreo y reporte, que ayuden a la detección de traspaso a la seguridad.
    - Establecer la política interna de TI que regule el comportamiento, describa los roles, responsabilidades y rutas para la rendición de cuentas de cada una de las personas.
    - Establecer un procedimiento que asegure que todos los usuarios conozcan y se comprometan a cumplir las políticas enfocadas a la protección de los activos de información y recursos tecnológicos de la organización. Al inicio de la relación se podría normar la firma de un documento formal y legal donde se exprese el compromiso de cumplimiento.

- Alteración de la integridad de la información
    - Incentivar la figura de propietario de datos y dueño de sistemas de información a los responsables de la información en el negocio. Proveerles los procedimientos y herramientas que faciliten su labor.

- Establecer el procedimiento para los requerimientos de cambio. Se deben incluir los cambios en aplicaciones, procedimientos, procesos, sistemas, cambios en configuraciones de componentes de infraestructura de hardware y software. Tales cambios deben ser aprobados, categorizados y priorizados.
- Crear y mantener la información de todos los activos de TI que incluya su clasificación e interrelación.
- Definir y establecer un procedimiento para realización de respaldos y recuperación de información. El procedimiento debe especificar la clasificación de la información que se incluye y excluye, así como el tiempo que estará disponible.

- Exposición de la información
  - Definir la política que la información sensible se puede trasladar únicamente por el medio estándar autorizado y aprobado por el negocio.
  - Definir la política acerca del uso de internet, correos electrónicos personales y uso de dispositivos externos que tienen posibilidad de conectarse a la red interna.
  - Establecer un procedimiento que asegure que todos los usuarios conozcan y se comprometan a cumplir las políticas enfocadas a la protección de los activos de información y recursos tecnológicos de la organización. Al inicio de la relación se podría normar la firma de un documento formal y legal donde se exprese el compromiso de cumplimiento.
  - Establecer el mecanismo de protección a los activos de información que se encuentran en equipos estacionarios y especialmente a los móviles que tienen mayor exposición.

5.3.3.5. Riesgos en las aplicaciones en TI

- Incorrectas decisiones de inversión en aplicaciones
  - Implementar un comité de IT que se encargue de priorizar los programas de inversión para que estén alineados con la estrategia de la organización.
  - Establecer el compromiso con los interesados. Se debe obtener el compromiso y participación de los actores involucrados en la definición y ejecución de las actividades del proyecto.
  - Establecer la política interna de TI que regule el comportamiento, describa los roles, responsabilidades y rutas, para la rendición de cuentas de cada una de las personas.
  - Establecer métricas, reportar a los interesados y monitorear los resultados de los proyectos. Enfocarse en aspectos de cronograma, costo y calidad. Identificar las desviaciones y el impacto en los resultados.
  - Comprender la demanda actual y futura del recurso humano y conocer las habilidades que serán necesarias para alcanzar los objetivos y asegurar su disponibilidad, lo cual involucra no tener ni excedentes ni faltantes.

- Envejecimiento de las aplicaciones de negocio
  - Fomentar la estandarización tecnológica.
  - Establecer la dirección para la planificación tecnológica.
  - Diseñar la estrategia que permita mantener las aplicaciones de software. Evaluar periódicamente las aplicaciones para implementar mejoras en diseño y funcionalidad.
  - Evaluar la capacidad actual y el rendimiento de las soluciones entregadas y comparar con las necesidades futuras.

- Implementación inadecuada de las aplicaciones
    - Implementar en la fase de planificación, la especificación y puntos de control para alcanzar la calidad esperada en los proyectos.
    - Planificar y ejecutar la transferencia de conocimiento para el personal operativo y de soporte.
    - Establecer un plan de implementación y de contingencia del proyecto aprobado por los interesados.
    - Asegurar que los dueños del proceso de negocio, personal de TI e interesados, evalúen y aprueben el resultado de las pruebas del software de acuerdo con el plan de pruebas establecido.

- Inestabilidad de las aplicaciones
    - Desarrollar la estrategia que permita el adecuado mantenimiento de las aplicaciones de software.
    - Monitorear periódica y continuamente el rendimiento y la capacidad de las aplicaciones y recursos de TI. Es útil para asegurar el cumplimiento de los niveles de servicio esperados y para obtener el estado real de las aplicaciones.
    - Asegurar que los dueños del proceso de negocio, personal de TI e interesados, evalúen y aprueben el resultado de las pruebas del software de acuerdo con el plan de pruebas establecido.
    - Instituir el procedimiento para la administración de problemas. Se debe registrar la información necesaria para facilitar la trazabilidad del problema, detalle de errores, conocer las causas, los recursos afectados, recursos utilizados, conocer el tiempo de los eventos y la solución ejecutada.

- Falta de capacidad de las aplicaciones
    - Monitorear periódica y continuamente el rendimiento y la capacidad de las aplicaciones y recursos de TI. Es útil para asegurar el cumplimiento de los niveles de servicio esperados y para obtener el estado real de las aplicaciones.
    - Realizar el mantenimiento de la infraestructura en forma periódica, según las recomendaciones de los fabricantes.

- Envejecimiento de las aplicaciones de infraestructura
    - Establecer la dirección para la planificación tecnológica.
    - Establecer un plan de adquisición que incluya el corto, mediano y largo plazo.
    - Realizar el mantenimiento de la infraestructura en forma periódica según las recomendaciones de los fabricantes.

- Aplicaciones intrusas
    - Establecer medidas para prevenir, detectar y corregir la intromisión de software malicioso. Planificar las actualizaciones de seguridad y mantener actualizado el antivirus corporativo.

5.3.3.6. Riesgos en los servicios que provee la TI

- Riesgos en la entrega y soporte de servicios
    - Establecer un procedimiento para selección de proveedores en forma justa y transparente. Adicionalmente, incluir el procedimiento que incluya creación, modificación y cancelación de contratos con proveedores.

- Establecer una normativa respecto de los acuerdos de servicios con los proveedores y los compromisos que sean adquiridos por ambas partes.
- Establecer contratos que sean apegados a las normativas internas y legales. Clarificar los términos de seguridad, sanciones o penalizaciones y premios.
- Normar el proceso que permita definir y colectar las métricas referentes al cumplimiento de los acuerdos de servicios, incluyendo aquellos que son provistos por los proveedores.

- Rendimiento de los servicios
  - Definir los acuerdos del nivel de los servicios como mínimo para aquellos que sean críticos, basados en la capacidad de TI y los requisitos de los interesados, quienes deberán estar en común acuerdo, respecto de la disponibilidad, fiabilidad, restricciones, seguridad, rendimiento, continuidad y tiempos de solución.
  - Diseñar un plan de recuperación y reanudación de servicios.
  - Establecer el proceso que permita definir y colectar las métricas referentes al cumplimiento de los acuerdos de servicios, incluyendo aquellos que son provistos por los proveedores.
  - Desarrollar y mantener un plan de continuidad; este debe incluir instrucciones claras para obtener la recuperación de todos los servicios críticos de TI, responsabilidades y procedimientos de comunicación.

5.3.3.7. Riesgos en el cumplimiento corporativo de TI

- Cumplimiento de acuerdos y compromisos
    - Establecer una normativa referente a los acuerdos de servicios con los proveedores y los compromisos que sean adquiridos por ambas partes.

- Cumplimiento de licenciamiento
    - Identificar las regulaciones locales e internacionales respecto de los cumplimientos de la propiedad intelectual y derechos sobre licenciamiento.
    - Establecer la política que prohíba el uso de software sin el licenciamiento debido. Incluir la especificación que regule el uso de software libre en la organización.

- Cumplimiento de regulaciones
    - Identificar las regulaciones locales e internacionales respecto de los cumplimientos de la industria, laborales y fiscales en la organización y que tengan relación con las políticas y procedimientos internos de TI.

5.3.3.8. Riesgos en el cumplimiento legal de TI

- Cumplimiento legal en Guatemala
    - Identificar las regulaciones locales e internacionales en relación con los cumplimientos de la industria, laborales y fiscales en la organización y que tengan relación con las políticas y procedimientos internos de TI.

- Las organizaciones en el medio guatemalteco deben clarificar los derechos de autor especialmente lo que se refiere al desarrollo de software o programas informáticos. Se sugiere que por medio de un documento escrito entre la organización y el programador de sistemas, se declaren los derechos de propiedad intelectual que ambas partes acuerden.

5.3.3.9. Otros escenarios de riesgos de TI

- Rendición de cuentas de TI
  - Establecer la política interna de TI que regule el comportamiento, describa los roles, responsabilidades y rutas, para la rendición de cuentas de cada una de las personas.

- Integración de TI y los procesos de negocio
  - Instituir el proceso que permita la educación bidireccional de la planeación estratégica de TI con el negocio.
  - Establecer mecanismos que faciliten la coordinación, comunicación e interacción entre personal de TI y las partes interesadas en el negocio.

- Procesos operativos de TI y manejo de errores
  - Establecer el procedimiento de entrenamiento apropiado para empleados nuevos y la formación continua para alcanzar los objetivos organizacionales.
  - Definir y documentar los procedimientos operacionales de TI.
  - Establecer un plan de recuperación y reanudación de servicios de TI.

5.4. Gestión de la comunicación

Indudablemente, la comunicación tiene un papel preponderante en el buen desempeño de cualquier organización y su importancia en la gestión de riesgos no es la excepción. La información además de ser colectada, organizada y estructurada, debe ser comunicada con eficacia a las personas correctas, en el momento adecuado.

En la práctica, las organizaciones pueden elegir entre diferentes opciones para hacer fluir la información a los interesados. Algunas de las prácticas más comunes para la transmisión de mensajes son: comunicación directa, utilizando teléfonos, correo electrónico, uso de carpetas compartidas en la red interna, impresión y distribución de documentos, realización de presentaciones en reuniones presenciales o remotas, distribución de información en medios electrónicos, utilización de herramientas colaborativas que centralizan la información, etcétera. El medio que se va a utilizar, dependerá en buena medida, de los recursos disponibles en la organización.

Las acciones que se sugiere realizar son las siguientes:

- Establecer un plan de comunicación que permita la disponibilidad de la información a las personas correctas, en el momento oportuno.
- Especificar a todos la forma en que fluye, los medios y la periodicidad con la que tendrán disponible la información.
- Clarificar los roles de cada involucrado, quienes crean, autorizan, modifican y leen la información.

5.5. Monitoreo y supervisión

El trabajo que conlleva la realización de las actividades relacionadas con la administración de riesgos de TI, deben estar sujetas a un proceso permanente de monitoreo y supervisión. El objetivo de esta práctica es velar porque el área de TI cumpla con las normativas internas y externas, ayudar a identificar mejoras en los controles implementados, evaluar los resultados de las métricas establecidas y monitorear que los riesgos se mantengan dentro del límite aceptado por el negocio.

Estas acciones en la práctica pueden ser realizadas por personal interno de TI, personal de auditoría interna, firmas de auditoría o su combinación. El realizar esta actividad permitirá:

- Evaluar si se ha alcanzado el nivel de madurez de la gestión de riesgos que se propuso inicialmente.
- Informar los resultados al nivel directivo de la organización y al responsable de TI.
- Obtener la información para el proceso de mejora continua.

5.6. Mejora continua

La mejora continua es un concepto que busca el perfeccionamiento continuo y sostenible que puede ser aplicado en la gestión de riesgos de TI.

Se ha utilizado este concepto para evaluar el estado actual de la organización, plantear el estado futuro que se desea alcanzar y determinar qué acciones se requieren para el cambio.

Posterior a implementar los cambios, se debe realizar una actividad de monitoreo y supervisión que permita evaluar los resultados que servirán de base para un nuevo proceso de mejora continua.

CONCLUSIONES

1. La gestión de riesgos de TI en las organizaciones sirve para evitar y minimizar pérdidas, pero también es útil para generar valor por medio de la aplicación de conceptos, principios y un conjunto de acciones definidas en controles.

2. Las empresas que poseen el nivel de sofisticación mediano o alto de TI son más dependientes de ella y crece su exposición a diversos riesgos, los cuales pueden comprometer el cumplimiento de los objetivos estratégicos. La respuesta a estos riesgos, involucra la implementación del proceso de mejora continua del nivel de madurez.

3. En el medio corporativo en Guatemala el nivel de madurez de la gestión de riesgos de TI es aceptable, considerando la manera en que se gestionan. Existen empresas que han implementado marcos de trabajo, estándares y metodologías para responder adecuadamente a los riesgos. No obstante, hay una oportunidad de mejora, ya que una cantidad significativa no le da la atención debida.

4. En el mercado nacional e internacional existen soluciones para la administración de riesgos corporativos y riesgos de TI. Con base en tales soluciones, se ha propuesto un marco de trabajo con enfoque práctico que especifica los pasos a seguir para implementar la mejora del nivel de madurez de la gestión de riesgos y que cubre los diferentes escenarios relacionados con TI.

RECOMENDACIONES

1. Las entidades y/o empresas deberán decidirse por el cambio de visión respecto de los riesgos e implementar una cultura de trabajo orientada a resolverlos y considerarlos como oportunidad de generación de valor, lo cual colaborará con alcanzar los objetivos estratégicos.

2. Se debe tomar conciencia de la exposición a diferentes escenarios de riesgo y ejecutar las acciones planteadas para mejorar el nivel de madurez de la gestión de riesgos, enfocándose inicialmente en aquellas áreas que son críticas y que tengan relevancia según los objetivos estratégicos.

3. Para un mejor aprovechamiento de los recursos y servicios de TI, las empresas en el medio corporativo en Guatemala deben darle mayor importancia a la administración de riesgos, realizar las acciones necesarias para su implementación y asegurar su cumplimiento por medio de actividades de control, comunicación y supervisión.

4. Existen opciones disponibles para la administración del riesgo corporativo de TI. Se debe hacer una evaluación objetiva para determinar cuál se adapta mejor al contexto propio y a los objetivos que se han trazado. Lo importante es tomar la iniciativa para el cambio y envolverse en un proceso de mejora continua tal como lo sugiere el marco de trabajo propuesto.

BIBLIOGRAFÍA

1. Clinch Consulting. *ITIL y la seguridad de la información* [en línea]. Disponible en Web: <http://www.best-management-practice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf> [Consulta: junio de 2011].

2. Congreso de Guatemala. Acuerdo de la Superintendencia de Administración Tributaria 24-2007 acerca del régimen optativo de factura electrónica [en línea]. Disponible en Web: <http://www.congreso.gob.gt/gt/mostrar_acuerdo.asp?id=17281> [Consulta: mayo de 2011].

3. _____. Decreto de ley 33-98 de Derechos de Autor y Derechos Conexos [en línea]. Disponible en Web: <http://www.congreso.gob.gt/gt/mostrar_ley.asp?id=789> [Consulta: mayo de 2011].

4. _____. Decreto de ley 47-2008 para el reconocimiento de las comunicaciones y firmas electrónicas [en línea]. Disponible en Web: <http://www.congreso.gob.gt/gt/mostrar_ley.asp?id=13080> [Consulta: mayo de 2011].

5. _____. Decreto de ley 56-2000 modifica la ley de Derechos de Autor y Derechos Conexos especificados en el Decreto 33-98 [en línea]. Disponible en Web: <http://www.congreso.gob.gt/gt/ mostrar_ley.asp?id=639> [Consulta: mayo de 2011].

6. _____. Decreto de ley 57-2000 de propiedad intelectual [en línea]. Disponible en Web: <http://www.congreso.gob.gt/gt/mostrar_ ley.asp?id=640> [Consulta: mayo de 2011].

7. _____. Decreto de ley 57-2008 acerca del acceso a información pública [en línea]. Disponible en Web: <http://www.congreso.gob.gt/gt/mostrar_ley.asp?id=13086> [Consulta: mayo de 2011].

8. COSO ERM. Gestión de riesgos corporativos [en línea]. Disponible en Web: <http://www.iaiecuador.org/downloads/ev_01/Coso%20ERM2.pdf> [Consulta: abril de 2011].

9. _____. Gestión del riesgo empresarial [en línea]. Disponible en Web: <http://www.coso.org/documents/COSO_ERM_Executive Summaryspanish.pdf> [Consulta: abril de 2011].

10. Engineers Australia. Estándar AS/NZS 4360 para gestión de riesgos [en línea]. Disponible en Web: <http://www.r2a.com.au/briefings/RES%20Qld%20presentation.pdf> [Consulta: mayo de 2011].

11. ENISA. European Network and Information Security Agency, Magerit metodología para análisis y gestión de riesgos [en línea]. Disponible en Web: <http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html> [Consulta: junio de 2011].

12. ERM. Gestión del riesgo empresarial [en línea]. Disponible en Web: <http://www.ccee.edu.uy/ensenian/catcoint/material/2da%20clase%20 riesgos Z-ERM-08.pdf> [Consulta: abril de 2011].

13. GRC. Gobierno, riesgo y cumplimiento [en línea]. Disponible en Web: <http://www.isacamty.org.mx/archivo/GRC.pdf> [Consulta: abril de 2011].

14. IEEE Standars Association. Estándar para la dirección de proyectos [en línea]. Disponible en Web: <http://standards.ieee.org/findstds/standard/1490-2003.html> [Consulta: junio de 2011].

15. ISACA. Guía profesional de riesgos de TI [en línea]. Disponible en Web: <http://www.isaca.org/Knowledge- Center/Research/Research Deliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx> [Consulta: marzo de 2011].

16. _____. Marco de trabajo de riesgos de TI [en línea]. Disponible en Web:<http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-framework-spanish.pdf> [Consulta: marzo de 2011].

17. ISACA COBIT. Marco de trabajo para gobierno y control de TI [en línea]. Disponible en Web: <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx> [Consulta: junio de 2011].

18. ISACA JOURNAL. Volumen 1 2010. El mínimo de controles de TI para evaluar en una auditoría financiera [en línea]. Disponible en Web: <http://www.isaca.org/Journal/Past- Issues/2010/Volume-/Pages/The-Minimum-IT-Controls-to-Assess-in-a-Financial- Audit-Part-I-1.aspx> [Consulta: junio de 2011].

19. ISO. Estándar ISO 31000:2009. Principios y directrices en la gestión de riesgos [en línea]. Disponible en Web: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170> [Consulta: mayo de 2011].

20. _____. Estándar ISO/IEC 27005:2011. Técnicas de seguridad para TI [en línea].Disponible en Web:<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56742> [Consulta: junio de 2011].

21. Registro Mercantil. Detalle de estadísticas desde el año 1999 al 2011 [en línea]. Disponible en Web: <http://www.registromercantil.gob.gt/estadisticas.asp> [Consulta: mayo de 2011].

22. Riesgos. Análisis de riesgos [en línea]. Disponible en Web: <http://revistas.concytec.gob.pe/pdf/id/v9n1/a13v9n1.pdf> [Consulta: abril de 2011].

23. Slideshare. Concepto de riesgo. [en línea]. Disponible en Web: <http://www.slideshare.net/cerodano/concepto-de-riesgo> [Consulta: marzo de 2011].

24. Wikipedia. Riesgo. [en línea]. Disponible en Web: <http://es.wikipedia.org/wiki/Riesgo> [Consulta: marzo de 2011].

APÉNDICE

1. Encuesta

Encuesta realizada y publicada en internet para reunir información sobre la gestión de riesgos de TI en el medio empresarial guatemalteco.

Objetivo: Conocer cómo las empresas en el medio guatemalteco gestionan los riesgos de TI (Tecnologías de la Información). Dirigida a personas que trabajan dentro de un departamento o área de informática.
Instrucciones: Por favor responda a las siguientes preguntas de acuerdo a lo que usted conoce dentro de su ambiente laboral. Tiempo estimado para llenar la encuesta de 3 a 5 minutos.

---

*Obligatorio

Perfil del encuestado

Desarrollo mis actividades laborales en una empresa u organización que provee de servicios o recursos de TI a la siguiente cantidad de usuarios (internos o externos): *

- Menos de 10 usuarios
- Entre 10 y 50 usuarios
- Más de 50 usuarios

Desarrollo mis actividades laborales en una empresa que pertenece al sector: *

- Privado
- Público

Preguntas

¿En la organización o empresa, existe alguien que administre los riesgos para toda la organización? *

- Sí
- No

- No sé

¿En la organización o empresa, existe alguien que administre los riesgos específicamente de TI? *

- Sí
- Si, es la misma que gestiona los riesgos en la organización
- No
- No sé

¿He escuchado en la organización o empresa acerca del inventario, portafolio o perfil de riesgos de TI? *

- Sí
- No

Indique cuál metodología, estándar, herramienta o marco de trabajo se utiliza para la gestión parcial o total de riesgos de TI: *

- COBIT
- ITIL
- ISO (Ej. ISO 31000, ISO 27002, u otro que pertenece a ISO)
- COSO ERM
- Risk IT
- Metodología a la medida o propia
- Se utiliza otra
- No se utiliza ninguna
- No sé

¿En la organización o empresa, existen normas, políticas o procedimientos que describen la manera en que se debe utilizar los recursos y servicios relacionados con TI? * Ejemplos: Procedimiento para solicitar accesos a los sistemas de información de la empresa, reglamento para el uso internet y correo electrónico, etc.

- Sí
- No
- Solo para algunos servicios o recursos

¿Conoce usted controles o mecanismos implementados en la organización que permiten identificar o alertar sobre la existencia de un riesgo relacionado con TI? * Ejemplos de riesgos de TI: Atraso en proyectos por personal interno, interrupción de servicios, accesos no autorizados a información, etc.

- Sí, controles manuales
- Sí, controles automáticos
- Sí, controles manuales y automáticos
- No hay controles
- No sé

¿Sabe usted qué acciones debe realizar cuando un riesgo de TI se presenta o está por materializarse en su área de trabajo, para que éste alcance el valor aceptado por el negocio? * Ejemplos de riesgos de TI: Atraso en entrega de proyectos por terceros, interrupción del servicio de electricidad, alteración de software e información en acciones fraudulentas, etc.

- Sí, existen acciones concretas definidas internamente
- Sí, conozco lo que se debe hacer aunque no estén definidas internamente
- Existen acciones definidas para casos puntales de alto impacto
- No sé

¿La organización o empresa, utiliza TI para la adquisición de beneficios y generación de valor a través de nuevos productos, servicios innovadores o nuevas oportunidades de negocio? *

- Si
- No
- No sé

Enviar