SATHIRÍ Sembrador

MODELO METODOLÓGICO BASADO EN RISK IT COMO ESTRATEGIA PARA LA GESTIÓN DE RIESGOS ORGANIZACIONALES

METHODOLOGICAL MODEL BASED ON RISK IT AS A STRATEGY FOR ORGANIZATIONAL RISK MANAGEMENT

Recibido: 26/01/2022 - Aceptado: 13/06/2022

SUYANA FABIOLA ARCOS VILLAGÓMEZ

Docente de la Pontificia Universidad Católica del Ecuador
Quito - Ecuador

Magíster en Gerencia de Sistemas
Universidad de las Fuerzas Armadas

sfarcos@puce.edu.ec
https://orcid.org/0000-0003-1088-1270

FREDDY MAURICIO TAPIA LEÓN

Docente de la Universidad de las Fuerzas Armadas
Sangolquí - Ecuador

Máster en Investigación e Innovación en Tecnologías de la Información y Comunicaciones
Universidad Autónoma de Madrid

fmtapia@espe.edu.ec
https://orcid.org/0000-0001-9591-3563

GUSTAVO XAVIER CHAFLA ALTAMIRANO

Docente de la Pontificia Universidad Católica del Ecuador
Quito - Ecuador

Doctor en Informática
Universidad Politécnica de Madrid

gxchafla@puce.edu.ec
https://orcid.org/0000-0003-4754-4446

DAMIÁN ANÍBAL NICOLALDE RODRÍGUEZ

Docente de la Pontificia Universidad Católica del Ecuador
Quito - Ecuador

Magíster en Redes de Comunicaciones
Pontificia Universidad Católica del Ecuador

danicolalde@puce.edu.ec
https://orcid.org/0000-0003-4999-2293

Cómo citar este artículo:

Arcos, S., Tapia, F., Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Resumen

El riesgo es la combinación de la probabilidad de que ocurra una calamidad y, además ,el resultado o el impacto de la misma cuando sucede. Tiene influencia sobre los objetivos que se ha planteado la organización porque puede desviarlos de lo planificado hacia positivo o hacia negativo. El riesgo y las oportunidades conviven, por lo que la gestión de ambos es una actividad estratégica clave para el éxito de la organización. Entonces, la gestión de riesgos es el proceso de identificar y aplicar medidas de control para contrarrestar los eventos riesgosos y, por consiguiente, proteger los activos de la organización mediante actividades aprobadas y coordinadas que lleven a la empresa a cumplir las metas propuestas. El presente trabajo propone una guía para la gestión de riesgos basada en la herramienta RISK IT de ISACA, herramienta aplicada a nivel global. Para cumplir con el propósito se desarrolló una metodología específica, basada en RISK IT. Dentro de la guía metodológica propuesta constan los ámbitos de gobernar el riesgo, evaluar y responder al mismo y además nueve procesos que van desde administrar el riesgo, recopilar datos, analizarlos, brindar una respuesta mediante controles y recomendar estrategias para comunicarlos y expresarlos de modo que se conviertan en parte de la cultura de riesgos organizacionales.

Palabras clave: *Gobernar el riesgo, evaluar el riesgo, responder al riesgo, gestión de riesgos de TI.*

Abstract

The risk is the combination of the probability of a calamity occurring and also the result of it when it happens. It has influence on the objectives that the organization has set because it can divert them from what was planned to positive or negative. Risk and opportunities coexist, so the management of both is a key strategic activity for the success of the organization. Then, risk management is the process of identifying and applying control measures to counteract risky events and therefore protect the organization's assets through approved and coordinated activities that lead the company to meet the proposed goals. This paper proposes a guide for risk management based on the ISACA RISK IT tool, a tool applied globally. To fulfill the purpose, a specific methodology was developed, based on RISK IT. Within the proposed methodological guide, there are the areas of governing risk, evaluating and responding to it, and nine processes that range from managing risk, collecting data, analyzing them, providing a response through controls, and recommending strategies to communicate and express them in a way that become part of the organizational risk culture.

Keywords: *Govern risk, assess risk, respond to risk, IT risk management.*

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Introducción

Gestionar riesgos es garantizar que se administren las medidas para aprovechar las oportunidades estratégicas de una organización que posee sistemas de información e infraestructura de TI y, además, de que se consiga una reducción del riesgo a un nivel aceptable. Un riesgo es una contingencia o proximidad de un daño. El concepto de riesgo ha tenido diversas interpretaciones, pero existe riesgo en cualquier situación en que no se conoce con exactitud lo que ocurrirá a futuro (RAE, 2019).

Las empresas, organizaciones e instituciones, públicas o privadas, al poseer infraestructura de tecnologías de información, realizan diferentes actividades relacionadas con su función, lo que las expone y enfrenta a diversos riesgos asociados, lo cual ha motivado la presente investigación en el contexto de proponer una guía metodológica basada en RISK IT como estrategia para la gestión de riesgos que se pueda adaptar a cualquiera de ellas. El marco metodológico RISK IT de ISACA se diferencia de otros marcos o modelos de riesgos, debido a que mientras la mayoría de aquellos busca eliminar los riesgos, RISK IT "considera la posibilidad de ir en la búsqueda de riesgos que, gestionados, podrían beneficiar a la organización, siempre que se encuentre el balance adecuado entre riesgo y valor" (ISACA, 2020, pág. 7).

Una guía metodológica como la propuesta, al ser aplicada, permitirá identificar y tener conocimiento sobre los peligros e incidentes que surgen a partir de las acciones empresariales, mismos que pueden tener un efecto tanto negativo como positivo en el éxito de toda organización. Un cargo directivo o gerencial en una empresa, al adoptar una metodología de gestión de riesgos y mantenerla vigente con cierta periodicidad podría beneficiarse de aspectos relacionados con el conocimiento global y específico oportuno sobre los riesgos a los que están expuestos los activos tecnológicos bajo su administración y por consiguiente tener la posibilidad de tomar decisiones de manera consiente e informada.

Por lo tanto, en la presente investigación se ha desarrollado una guía metodológica que abarca, en sus etapas, las buenas prácticas que propone RISK IT como herramienta utilizada a nivel global para gestionar riesgos.

Materiales y métodos

La contextualización del estudio es exploratoria. Los estudios exploratorios se realizan cuando el objeto es examinar un tema a profundidad y este problema de investigación ha sido poco estudiado o no se ha abordado antes (Hernández, Fernández & Baptista, 2010). El estudio se llevó a cabo a través de investigación bibliográfica donde los datos obtenidos pueden ser cualitativos y cuantitativos.

En primer lugar, se definieron los conceptos bajo los cuales se aborda la problemática de la gestión de riesgos como son seguridad de la información, vulnerabilidades, amenazas, ataques, impacto y riesgo. Dando lugar al cálculo de este para plantear su posterior tratamiento.

Después, se analizó la herramienta o instrumento RISK IT de ISACA especificando sus ámbitos y sus procesos. En consecuencia, se generó la propuesta de una guía metodológica como estrategia para la gestión de riesgos, describiéndose cada una de las etapas y en cada una de ellas se desarrolló el insumo apropiado.

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Resultados y discusión

En el contexto de la seguridad de la información, los sistemas informáticos y la infraestructura, se pueden definir conceptos de vulnerabilidad, amenaza, ataque e impacto (Yunn, 2019).

La seguridad es la protección brindada a un sistema de información automatizado para alcanzar los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información esto incluye hardware, software, firmware, información, datos y telecomunicaciones (NIST, 2018).

Así también, una amenaza es un problema potencial sobre la seguridad de un activo y una vulnerabilidad es una debilidad que puede hacer que una amenaza se vuelva una realidad o se materialice. Es una circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor (Instituto Nacional de Ciberseguridad, 2017).

Un ataque es una amenaza que se lleva a ejecución tomando provecho de las vulnerabilidades y puede ser de naturaleza intencionada tal como ataques lógicos a los sistemas de información con propósito destructivo y puede tomar forma de vandalismo; o pueden existir ataques de naturaleza no intencionada como un incendio accidental, una inundación por condiciones del clima, etc. (Erreyes, 2017).

Con lo dicho anteriormente, el impacto es la consecuencia o efecto de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. Generalmente, el impacto se suele medir o estimar en términos de porcentaje de degradación que afecta a un activo y el 100% sería la pérdida total del activo (Instituto Nacional de Ciberseguridad, 2017).

En consecuencia, el riesgo es la combinación de la probabilidad de que ocurra un evento y además el resultado cuando sucede. Tiene influencia sobre los objetivos que se ha planteado la organización porque puede desviarlos de lo planificado.

Al respecto, el Instituto Nacional de Ciberseguridad de España (INCIBE) indica que la forma de medir el nivel de riesgo es una estimación de lo que puede ocurrir y se valora de forma cuantitativa, como la consecuencia del impacto asociado a una amenaza por la probabilidad de ocurrencia de la misma, como se indica en la Figura 1:

Figura 1. Cálculo del Riesgo
Fuente: Instituto Nacional de Ciberseguridad (2017).

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

En resumen, se es vulnerable tanto como se carezca de protección suficiente para evitar que una amenaza llegue a materializarse. Un ataque es una amenaza que se ejecuta aprovechando una vulnerabilidad y el impacto es lo que se puede medir producto de la ocurrencia de un ataque.

ISACA define que gestionar riesgos es garantizar que se administren las medidas para aprovechar las oportunidades estratégicas de una organización que posee sistemas de información e infraestructura de TI y, además, que se consiga una reducción del riesgo. Un riesgo es una contingencia o proximidad de un daño (ISACA, 2020).

Es propicio recalcar que RISK IT es un marco o modelo, no una norma, lo que significa que cada organización debe personalizar los componentes que constan en el marco para adaptarlos a la organización. Pero el riesgo y la oportunidad conviven y la gestión de los dos es una actividad estratégica clave para el éxito de la organización.

RISK IT propone, mediante la gestión de riesgos de TI, un modelo que se divide en tres ámbitos o dominios y cada uno contiene tres procesos:

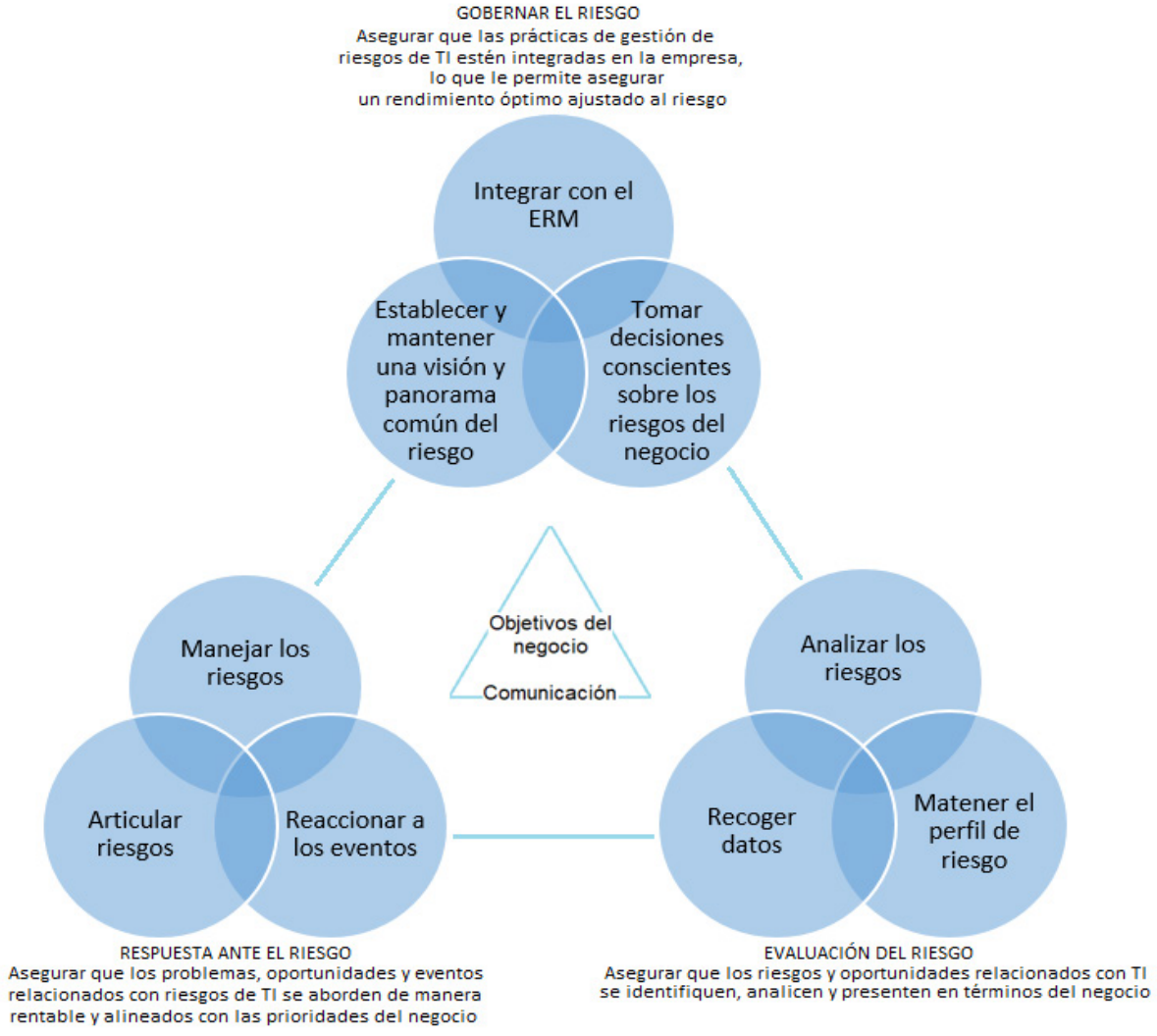

Figura 2. Estructura del Marco o Modelo de Riesgos de TI
Fuente: ISACA (2020).

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

En la Figura 2 se muestran los ámbitos de RISK IT, que son gobernar el riesgo, evaluación del riesgo y respuesta ante el riesgo y además se muestran los procesos que son: establecer y mantener una visión o panorama común del riesgo, integrar con el ERM o con la gestión de riesgos empresariales, tomar decisiones conscientes sobre los riesgos del negocio, recoger datos, analizar los riesgos, mantener el perfil de riesgo, articular riesgos y manejar riesgos. Tanto los ámbitos como los procesos constituyen la base de la estructura del marco o modelo de gestión de riesgos de RISK IT.

En base a la herramienta RISK IT, en la Figura 3 se muestra la metodología propuesta como estrategia para la gestión de riesgos. A continuación, se describen los ámbitos y sus respectivos procesos.

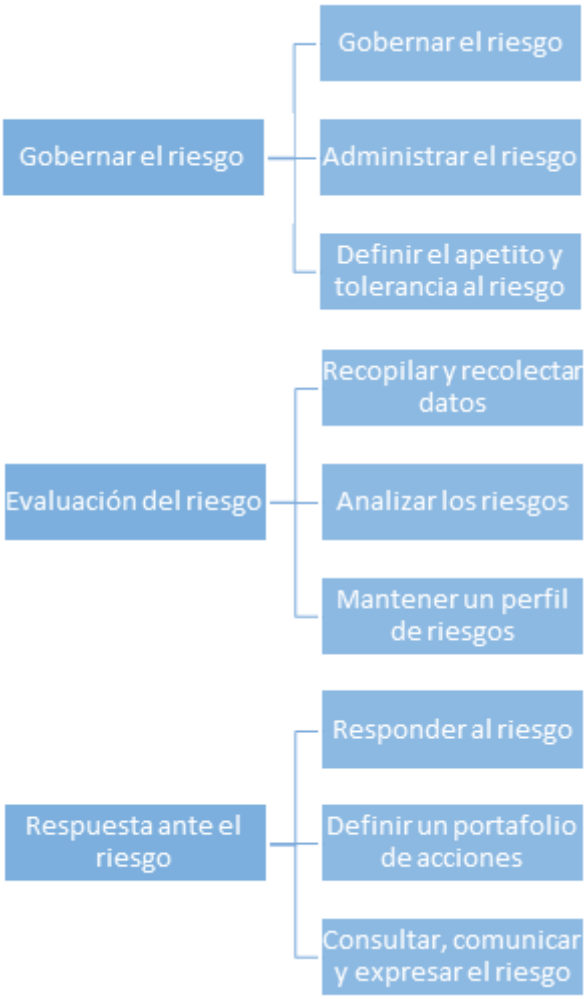

Figura 3. Marco o Modelo de Riesgos de TI como Metodología Propuesta

Ámbito 1. Gobernar el riesgo

Proceso 1. Gobernar el riesgo. "El término gobernar ha pasado a estar a la vanguardia del pensamiento empresarial como respuesta a algunos hechos que han demostrado la importancia de un buen gobierno" (Chambi, 2018, pág. 78). Se debe gobernar de forma integral, procurando

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

la creación de valor que es una de las asignaciones de los cargos de gobierno de la empresa, orientando este esfuerzo hacia satisfacer las necesidades de las partes interesadas.

La herramienta RISK IT indica que el éxito del gobierno corporativo radica en que existen grados o niveles de uso estratégico que se les puede dar a las TIC y que estas apalancan los recursos de la empresa para reducir el riesgo global, pero para ello se necesitan políticas y estas deben partir de la dirección o gobierno empresarial. Con lo cual, el punto de partida para iniciar el proceso de gestión de riesgos de TI debe ser contar con políticas para todas las dimensiones de la empresa que son generadas desde el ámbito de gobierno que se encarga de evaluar, orientar y supervisar (ISACA, 2020).

La responsabilidad de gobernar el riesgo debe recaer sobre el rol consignado específicamente para realizar esta actividad, RISK IT propone varias figuras como el Director Ejecutivo (Chief Executive Officer CEO, que es el más alto rango que se encarga de la gestión de la organización); el Director de Riesgo (Chief Risk Officer CRO, que supervisa los aspectos de gestión de riesgos de la organización); y el Responsable de Información (Chief Information Officer CIO, que es el responsable de las tecnologías de la información). Con cualquier denominación, este cargo debe asegurar que la actividad de gestión de riesgos se alinea con la capacidad objetiva de la empresa y el liderazgo de la misma, según lo que indican las pautas de RISK IT.

La política de gestión de riesgos tecnológicos deberá concebirse y documentarse al menos con los siguientes elementos:

- Objetivo de la política: el objetivo general debe orientarse a sensibilizar a los propietarios o encargados de los procesos y responsables de las TI sobre la existencia de los riesgos y la necesidad de minimizarlos oportunamente para mantenerlos dentro de los rangos aceptados por la organización como manejables en el contexto establecido dentro del apetito y tolerancia al riesgo.

- Responsables de la ejecución: deberá definirse el cargo encargado de la gestión de riesgos y el equipo encargado para cada área en particular, sus funciones sobre los procesos asignados, las actividades y el resultado esperado; y si existieran, deberá establecerse las jerarquías para definir líneas de comunicación apropiadas.

- Marco normativo: las organizaciones y empresas están regidas por normas y regulaciones. Es propicio que las mismas se identifiquen, sobre todo las que tengan relación con la gestión de riesgos. Estas pueden ser de carácter externo como de índole interna o relacionadas con políticas de seguridad de la información, además políticas de uso de recursos informáticos, etc.

- Descripción del marco metodológico: deberá identificar las pautas adoptadas para la gestión de riesgos, en el caso específico de este estudio se ha propuesto la incorporación de RISK IT con las adaptaciones particulares para la organización o empresa.

- Incumplimientos y situaciones no contempladas: deberá definirse el procedimiento para actuación en el caso de incumplimiento de la política establecida en la eventualidad de ocurrir un evento de riesgo y acontecimientos que no hayan sido contemplados (Gualim, 2014).

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Proceso 2. Administrar el riesgo. Administrar implica utilizar los recursos disponibles en la empresa para planificar acciones que ayuden a conseguir los objetivos planteados, en cambio; gestionar es poner en marcha lo planificado durante la administración. En las organizaciones, la administración es responsabilidad de los ejecutivos a cargo del Director General (CEO). Las áreas de responsabilidad son planificar, construir, ejecutar y supervisar. (ISACA, 2020)

La responsabilidad de administrar el riesgo recae sobre el rol consignado específicamente para realizar esta actividad, RISK IT propone la figura del Comité de Riesgos (conformado por los ejecutivos que son los responsables de las áreas de la empresa para apoyar las actividades de gestión de riesgos). (ISACA, 2020)

En la práctica, la administración de riesgos está relacionada con la definición de actividades para gestionar riesgos, implica un plan y el procedimiento como tal. Según los lineamientos de RISK IT los responsables de esta actividad deben integrar la estrategia de riesgos de TI y operaciones con la estrategia de riesgo de la organización (ISACA, 2020).

Administrar el riesgo contempla incluir los siguientes elementos:

- Procedimientos para identificar y evaluar el riesgo.
- Procedimientos para modificar y documentar la gestión de riesgos.
- Procedimientos para responder o tratar los riesgos.
- Procedimientos para realizar seguimiento y control de riesgos.
- Procedimientos para comunicar riesgos (Gualim, 2014).

Proceso 3. Definir el apetito y la tolerancia al riesgo. El apetito al riesgo se puede definir en términos de combinaciones entre frecuencia (probabilidad de ocurrencia) e impacto de un riesgo, factores a los que la organización se enfrenta para alcanzar una meta, prestando atención a lo que cada empresa haya definido como oportunidad, riesgo aceptable, riesgo elevado o riesgo inaceptable.

Según RISK IT, el apetito se puede definir mediante mapas de riesgos para definir la importancia de los mencionados riesgos según se posicionen en las bandas de colores definidas y además para establecer qué está permitido y qué no dentro de una organización. Internamente, en los mapas de riesgos se establece la combinación entre la frecuencia (probabilidad de ocurrencia) de un riesgo y el impacto de este (ISACA, 2020):

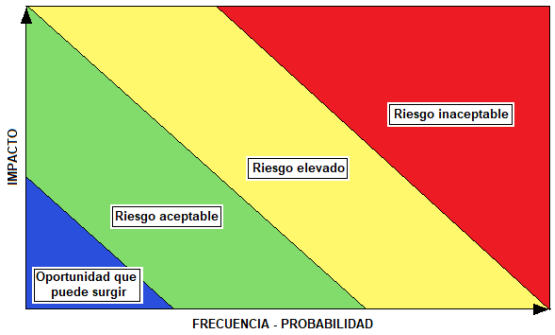

Figura 4. Bandas para mapas de riesgos
Fuente: ISACA (2020).

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

En la Figura 4 se distinguen bandas de colores, el rojo indica que un riesgo va más allá de su apetito por el riesgo definido como normal. El color amarillo indica que el riesgo es elevado pero la organización podría aceptarlo, aunque requiere una respuesta adecuada. El color verde indica un nivel normal aceptable de riesgo y para el que no se necesita acción. Por último, el color azul que es donde las oportunidades para asumir más riesgos pueden surgir (ISACA, 2020).

La tolerancia al riesgo es la variación o desviación aceptable en relación con la consecución de una meta y parte desde el nivel establecido por la definición del apetito al riesgo (ISACA, 2020).

En resumen, el apetito al riesgo indica la magnitud de riesgo que la organización está dispuesta a afrontar para alcanzar una meta y la tolerancia indica hasta dónde se podría aceptar una variación de esa magnitud para conseguir la misma meta después de haber sucedido un evento riesgoso.

Ámbito 2. Evaluación del riesgo

Proceso 4. Recopilar y recolectar datos:

- Identificar los Activos de Información:

Un activo es cualquier objeto de valor de la organización que puede ser afectado por un evento y crear un impacto en el negocio (ISACA, 2020, pág. 26).

Un activo necesita ser gobernado y gestionado y esto repercute sobre la información, los servicios, la infraestructura, las aplicaciones, los colaboradores, sus habilidades y competencias, etc. (ISACA, 2020).

Para la herramienta RISK IT los activos o recursos incluyen (ISACA, 2020):

- La gente o el recurso humano de la organización.
- Los servicios.
- Los activos físicos o la infraestructura de TI.
- Los recursos de software (ISACA, 2020).

Por todo lo anotado anteriormente, se ha realizado la siguiente clasificación de activos para que se sujete a los parámetros antes descritos:

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Tabla 1.
Clasificación de activos

TIPO DE ACTIVO	Descripción	NOMBRE DEL ACTIVO	Descripción
Activos Físicos	Hardware, equipamiento informático, equipos de comunicaciones, equipos técnicos, mobiliario	Nombre del Activo Físico	Servidores, equipos de escritorio, computadores portátiles, equipos celulares, impresoras, escáneres, firewall, switch, router, hub, central telefónica, dispositivos de VoIP, módem, red WiFi, red LAN, medios de almacenamiento extraíble, proyectores
Servicios	Que se prestan	Nombre del servicio que se presta	Servicios informáticos, servicios tecnológicos, servicios de comunicaciones, servicios de administración de cuentas, aprovisionamiento y administración, conectividad entre equipos y usuarios, navegación, monitoreo de la infraestructura, monitoreo, del acceso a servicios, cableado, instalación, soporte técnico, mantenimiento, atención en call center, plataforma, gestión de garantías, toma de huellas y generación de credenciales, préstamo portátiles, impresión.
	Que se necesitan para gestionar información	Nombre del servicio para gestionar información	Base de datos, cumplimiento de licenciamiento, cumplimiento de acuerdos y compromisos, cumplimiento de parámetros de seguridad, cumplimiento legal, nube, código ejecutable, código fuente
Recursos de Software	Software de aplicaciones, software libre, software especializado, software estándar, lenguajes de programación, sistemas operativos, herramientas de desarrollo, herramientas de publicación de contenido, utilitarios	Nombre del Activo de Software	Paquetes ofimáticos, cliente de correo electrónico, sistemas operativos, antivirus, sistema de respaldos, gestor de base de datos

Fuente: ISACA (2020).

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Proceso 5. Analizar los riesgos. Una vez que se cuenta con el inventario de activos de información se procede a analizar los riesgos o desarrollar información útil para apoyar las decisiones que se toman en torno a los riesgos. Se realiza lo siguiente:

a) Verificar los escenarios de riesgos:

Según RISK IT uno de los desafíos para gestionar riesgos entre todo lo que puede relacionarse con TI es la identificación de escenarios de riesgos debido a que permiten dar realismo a una situación, además de una estructura contextualizada de los riesgos y una visión amplia para poder mejorar el entorno completo. Una vez que se desarrollan estos escenarios se debe definir la probabilidad de frecuencia de la situación riesgosa y la estimación de los impactos para la organización (ISACA, 2020).

A continuación, en la Tabla 2, se muestran los ámbitos o categorías de los escenarios de riesgo y además los escenarios de riesgos que los conforman y que propone la herramienta RISK IT (ISACA, 2020):

Tabla 2.
Ámbitos o categorías y escenarios de riesgos de RISK IT

ÁMBITO DEL ESCENARIO DE RIESGO		ESCENARIO DE RIESGO	
A	INFRAESTRUCTURA DE TI	01	Obsolescencia de la infraestructura de TI
		02	Daño o destrucción de la infraestructura de TI
		03	Robo a infraestructura de TI
		04	Arquitectura de infraestructura de TI inadecuada
		05	Instalación y aplicación de cambios en infraestructura de TI
B	RELACIONADOS AL PERSONAL DE TI	06	Ausencia de personal clave de TI
		07	Falta de habilidades y experiencia del personal de TI
		08	Insuficiencia de personal clave de TI
C	GESTIÓN DE PROYECTOS DE TI	09	Proyectos no finalizados
		10	Riesgo económico de proyectos
		11	Retraso en la entrega de proyectos
		12	Baja calidad en los proyectos
		13	Falta de visión del portafolio de proyectos
D	GESTIÓN DE SEGURIDAD DE TI	14	Ataques lógicos a la seguridad
		15	Transgresión de seguridad
		16	Alteración de la integridad de la información
		17	Exposición de la información

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

E	APLICACIONES DE TI	18	Decisiones incorrectas de inversión en aplicaciones de TI
		19	Caducidad de las aplicaciones
		20	Implementación inadecuada de aplicaciones
		21	Inestabilidad de las aplicaciones
		22	Falta de capacidad de las aplicaciones
		23	Caducidad de aplicaciones de infraestructura
		24	Aplicaciones intrusas
F	ENTREGA Y SOPORTE EN LOS SERVICIOS QUE PROVEE TI	25	Entrega y soporte de servicios de TI
		26	Rendimiento de servicios
G	CUMPLIMIENTO CORPORATIVO DE TI	27	Cumplimiento de acuerdos y compromisos
		28	Cumplimiento de licenciamiento
H	CUMPLIMIENTO LEGAL DE TI	29	Cumplimiento legal de TI (en el país)
I	OTROS ESCENARIOS DE RIESGOS DE TI	30	Rendición de cuentas de TI
		31	Integración de TI y procesos de la organización
		32	Procesos operativos de TI y de manejo de errores

Fuente: (ISACA, 2020)

b) Realizar mapas de riesgos:

Con los escenarios definidos, lo que RISK IT recomienda a continuación, es realizar una evaluación probabilística de que ocurra un riesgo (la frecuencia) y además la consecuencia de este (el impacto) para verificar si estos parámetros se encuentran dentro de lo aceptable; considerando que la organización debió haber definido con anticipación el apetito y la tolerancia al riesgo (ISACA, 2020).

En resumen, para el análisis de riesgos se parte de los escenarios de riesgos y se realiza la medición del impacto y la frecuencia de los mismos y para llevar estos conceptos a la práctica se utilizan mapas de riesgos (o matrices de riesgos). Los mapas de riesgos son el resultado de la evaluación y permiten detectar si los escenarios de riesgos son una herramienta que favorece la adopción de medidas para que los mencionados riesgos puedan ser minimizados, es decir, un mapa de riesgos asiste en la identificación de la acción de gestión de riesgos requerida (Gualim, 2014). Con lo anteriormente expuesto, se elaboró el siguiente mapa o matriz de riesgos, el mismo que tiene integrado las escalas de frecuencia e impacto de los riesgos y además las bandas de colores para los mapas que definen o delimitan el apetito frente al riesgo:

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Tabla 3.
Mapa o matriz de riesgos

MAPA O MATRIZ DE RIESGOS							
RIESGO = FRECUENCIA * IMPACTO							
IMPACTO	Desastroso o extremo	5	5	10	15	20	25
	Mayor o alto	4	4	8	12	16	20
	Moderado	3	3	6	9	12	15
	Menor o bajo	2	2	4	6	8	10
	Insignificante o leve	1	1	2	3	4	5
			1	2	3	4	5
			Remoto	Poco probable	Probable	Muy Probable	Esperado
			FRECUENCIA				

Cabe indicar que al valorar la frecuencia y el impacto se obtienen los riesgos inherentes y se ubican en el mapa de riesgos donde se muestra el nivel de exposición que la organización experimenta por cada riesgo. Un riesgo inherente también se lo llama intrínseco y es propio del trabajo o proceso de la organización. Se identifica antes de aplicar cualquier control (ISACA, 2020).

A continuación, se colocan los valores resultado de la matriz de riesgos, la banda de color a la que corresponden y su significado (o nivel) en el mapa o matriz de riesgos:

Tabla 4.
Riesgo calificado según niveles de bandas de colores

RIESGO CALIFICADO SEGÚN BANDAS DE COLORES				
Inaceptable	15	16	20	25
Elevado	8	9	10	12
Aceptable	3	4	5	6
Oportunidad	1	2		

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Proceso 6. Mantener un perfil de riesgos. Mantener un perfil de riesgo es el último componente dentro de la evaluación del riesgo, es aquí donde se debe mantener actualizado el inventario de los riesgos conocidos en los pasos anteriores en respuesta a cualquier cambio, además las categorías o los ámbitos con los que tienen relación, con criterios de frecuencia e impacto y escala según bandas de colores acorde al nivel de apetito al riesgo que corresponda en el contexto de la organización (ISACA, 2020). Para el presente estudio se desarrolló la tabla 5 donde se integran todos los criterios anteriores y son preliminares a la última etapa que es responder al riesgo.

Tabla 5.
Perfil de Riesgos

PERFIL DE RIESGOS							
IMPACTO	Desastroso o extremo	5					
	Mayor o alto	4					
	Moderado	3					
	Menor o bajo	2					
	Insignifican-te o leve	1					
			1	2	3	4	5
			Remoto	Poco probable	Probable	Muy Probable	Esperado
			FRECUENCIA				

En la matriz se deberá ubicar el activo y el escenario de riesgos que le afectó. Podría estar representado por un código único del activo y un código de escenario que convergen y se sitúan en una casilla de la matriz.

Ámbito 3. Respuesta ante el riesgo

Proceso 7. Responder al riesgo. Para responder al riesgo primeramente es necesario decidir si un riesgo puede tener un tratamiento específico o puede ser tratado durante el curso de procedimientos normalizados de gestión, es decir, integrar el tratamiento en las prácticas del día a día de la organización (Crespo, 2016).

En segundo lugar, se debe tener en cuenta lo que se quiere como deseable para el tratamiento de los riesgos para evitar, mitigar, compartir, aceptar o asumir el nivel de riesgo existente.

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Como tercera medida, se debe diseñar una opción de tratamiento preferente, por ejemplo, si el objetivo fuese evitar un riesgo la alternativa sería cambiar un proyecto o elegir procesos alternativos para convertir el riesgo en irrelevante; si lo que se decidió fue compartir un riesgo, la participación de un tercero como un asegurador podría ser una opción; y, a veces se requiere aceptar un riesgo debido a su baja probabilidad o consecuencias menores. Todas estas medidas deben ser cuidadosamente documentadas y evaluadas en relación a su viabilidad alrededor de la tolerancia al riesgo definida (Crespo, 2016).

Seguidamente, todas las opciones de tratamiento antes citadas pueden y deben ser combinadas con otros controles o contramedidas propias de la herramienta (RISK IT en este caso) y luego ser aplicadas según la dotación de recursos y otras consideraciones que hayan sido aprobadas.

Se debe tomar en cuenta que las contramedidas o catálogos de controles pueden variar con los avances de la tecnología, se pueden ir modificando, van desapareciendo, aparecen nuevos o evolucionan (ISACA, 2020).

La herramienta RISK IT asigna una medida o respuesta al riesgo (o tratamiento) por cada nivel de riesgo (o banda de colores) en el que se haya ubicado el mismo, lo que se explica en la siguiente tabla:

Tabla 6.
Respuesta al riesgo acorde al nivel de riesgo

NIVELES DE RIESGO	RESPUESTA AL RIESGO	DESCRIPCIÓN
Inaceptable	Evitar	La organización debe estimar que este nivel de riesgo va más allá de su apetito de riesgo normal. Cuando un riesgo se juzga inaceptable también entra en la categoría de evasión. Evadir o evitar un riesgo significa salir de las actividades o condiciones que dan cabida a ese riesgo. Evitar se aplica cuando no existe otra respuesta adecuada o cuando no existe ninguna respuesta rentable que pueda tener éxito en la reducción de la frecuencia y magnitud o cuando el riesgo no pueda ser compartido o transferido.
Elevado	Mitigar / Compartir	La mitigación significa se consigue con la introducción de medidas de control que intenten reducir la frecuencia de un suceso adverso y/o el impacto del evento en caso de que suceda. Además, el riesgo se puede compartir o transferir, significa reducir la frecuencia o impacto mediante la transferencia o distribución de una porción del riesgo. Las estrategias incluyen tener un seguro para incidentes relacionados con TI, la subcontratación de parte de las actividades de TI o establecer proyectos compartidos con un proveedor a través de acuerdos de inversión compartida.
Aceptable	Aceptar	Indica un nivel aceptable o normal de riesgo con ninguna acción requerida excepto el mantenimiento de controles actuales. Aceptar significa que cuando un riesgo en particular se produce la pérdida sea aceptada. Esto difiere de ignorar el riesgo porque aceptar supone que el riesgo es conocido.
Oportunidad	Asumir	Indica la existencia de un riesgo donde el ahorro de costo de oportunidad se puede encontrar al disminuir el grado de control o donde las oportunidades para asumir más riesgos pueden surgir

Fuente: ISACA (2012).

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Proceso 8. Definir un portafolio de acciones. Para definir un portafolio de acciones concretas se deben recomendar controles adecuados para minimizar los riesgos identificados; evitar, mitigar, aceptar o asumir el impacto de los mismos en el ámbito técnico. Esto implica la adecuación de controles o contramedidas a ser implementadas como tratamiento de los riesgos. La herramienta RISK IT tiene un portafolio de ciento dieciséis controles para cada uno de los escenarios de riesgos (ISACA, 2020). Se deben escoger los controles que se ajusten al activo determinado en el inventario según el escenario que esté influenciando sobre el mencionado activo.

Una vez implementados los controles se hace necesario el monitoreo y revisión de los cambios efectuados, la frecuencia de estas revisiones corresponde al nivel de riesgo que se identificó, la robustez de los controles que se adecuaron y la habilidad que se desarrolle al tratarlos para monitorear que las contramedidas estén funcionando de forma adecuada.

En este punto del proceso podría ser útil el cálculo del riesgo residual (posterior a la implementación de controles) y compararlo con el riesgo inherente (anterior a la implementación de controles), de manera que se observen los efectos posteriores de las acciones para el tratamiento de los riesgos (Cruces & Mora, 2016). De manera que la gestión de riesgos, en su integralidad corresponda a un proceso de mejora continua.

Proceso 9. Consultar, comunicar y expresar. Los riesgos deben ser dados a conocer a las partes interesadas. Comunicar y además consultar es esencial para que los responsables de la implementación de la gestión de riesgos puedan comprender los criterios sobre los que se toman decisiones y las razones del tratamiento de los riesgos en particular (ISACA, 2020). Comunicar y expresar los riesgos forma parte de la cultura de riesgos que posee la empresa donde se ofrece un entorno en donde los componentes de riesgos se discuten abiertamente, es decir, que los riesgos se conocen y se entienden.

RISK IT señala que existen algunos beneficios alrededor de la sensibilización y comunicación sobre riesgos dentro de la organización:

- Contribuye a la gestión ejecutiva para la comprensión de la exposición a los riesgos.
- Establece un comportamiento hacia las políticas que se tomen en el ámbito de los riesgos.
- Provee de transparencia a las partes interesadas en la toma de decisiones sobre riesgos.
- Establece un comportamiento hacia los resultados negativos, es decir, acontecimientos de pérdidas u oportunidades perdidas con el fin de adaptarse y tomarlos como situaciones aprendidas (ISACA, 2020).

Los métodos de comunicación y consulta podrían ser reuniones, reportes, sistemas de comunicación en línea, talleres de inducción y capacitación, grupos focales. El cargo o equipo encargado de esta tarea deberá tener como objetivos:

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

- Establecer el contexto y antecedentes de los riesgos.
- Asegurar que las expectativas de los interesados sobre el manejo o gestión de riesgos sean conocidas.
- Asegurar que los riesgos han sido correctamente identificados.
- Comunicar la asignación y tratamiento o respuesta para los riesgos.
- Comunicar las mejoras logradas asociadas a la gestión de riesgos (Gualim, 2014).

Conclusiones

- Una vez realizado el estudio se puede deducir que un riesgo es el efecto de la incertidumbre; la combinación de la probabilidad de un evento riesgoso y su ocurrencia e implica pérdida o afectación. Entonces, la gestión de riesgos se desarrolló con el propósito de proteger los activos y la información en pos de conseguir los objetivos y metas de la organización o empresa; a través de la identificación de eventos potenciales de riesgo y la inclusión de actividades coordinadas para dirigir, controlar y proteger a la organización con respecto al riesgo. Por lo tanto, se puede concluir que la gestión de riesgos establece estrategias para que las empresas sean capaces de absorber perturbaciones sin alterar significativamente su estructura y funcionalidad.
- Luego de haber culminado con la revisión de varios marcos, modelos y metodologías de gestión de riesgos desarrolladas y vigentes actualmente para finalmente escoger la herramienta RISK IT, se puede concluir que existen etapas o fases que describen una metodología integral; iniciando con el establecimiento del contexto, la identificación de los riesgos, la evaluación y valoración de los mismos y el plan específico de tratamiento. Con lo cual, se puede colegir que todas aquellas fases citadas, finalmente conducen a la evasión, reducción, compartición o retención de los riesgos, todas estas opciones de tratamiento deben ser evaluadas por su alcance, su costo y los beneficios derivados para la organización o empresa.
- Algunos de los componentes que pertenecen al ámbito gobernar el riesgo son las nociones de apetito ante el riesgo y tolerancia por el riesgo que son conceptos diferentes. El apetito por el riesgo está relacionado con la cantidad o magnitud de riesgo que la organización está dispuesta a aceptar para alcanzar una meta, mientras que la tolerancia al riesgo es la variación desde el nivel establecido por el apetito para conseguir la misma meta después de haber sucedido un evento riesgoso. Con lo expuesto, se puede concluir que son conceptos distintos, pero están relacionados complementariamente y dependen de las políticas que los directivos de las organizaciones hayan establecido y por lo tanto existirán tantos niveles de apetito y tolerancia al riesgo como organizaciones que decidan adoptar estos conceptos en su cultura de riesgos y llevarlos a la práctica.

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

- Al determinar los activos, las categorías de riesgos y los escenarios de riesgos a los que están expuestos los activos, se debe realizar una valoración de riesgos sobre los mismos, dando como resultado un número que se obtiene del cálculo de la probabilidad (frecuencia) de ocurrencia de un riesgo por el impacto que ese riesgo causa sobre un activo; este proceso es necesario para que el valor pueda ser plasmado en un mapa de riesgos debido a que este es un instrumento con utilidad en la identificación de una acción de gestión de riesgos requerida. Se puede concluir que, para optimizar recursos, antes de que ese valor sea plasmado en un mapa de riesgos se podría priorizar o escoger los valores de riesgos altos debido a que eso significa que el activo está más expuesto y necesita mayor atención.

- Posteriormente a determinar los activos de la organización, las categorías, los escenarios de riesgos, realizar la valoración de los riesgos y plasmar los mapas de riesgos; RISK IT sugiere mantener un perfil de riesgos conocidos actualizado. El perfil de riesgos es la última etapa de la evaluación del riesgo y por lo tanto se puede concluir que permite prepararse a la siguiente fase que es la respuesta ante el riesgo.

- Concluidas las etapas de gobernar el riesgo y evaluación del riesgo se debe responder al riesgo. Responder al riesgo implica brindar un tratamiento en torno a evitar, mitigar o compartir, aceptar y asumir los riesgos. Las opciones de tratamiento antes citadas pueden ser combinadas con otros controles o contramedidas. En conclusión, algunos activos de la empresa se ubicarán en niveles de riesgo inaceptables donde el tratamiento adecuado es evitar, otros activos se colocarán en niveles elevados de riesgo, con lo cual, se deberá mitigar/compartir, otro grupo de activos estarán menos expuestos y se situarán en un nivel aceptable de riesgo y el resto de los activos significarán una oportunidad, es donde se debe asumir ese riesgo como aprovechable. RISK IT, es la única herramienta de gestión de riesgos encontrada que posee esta característica, que viene a ser enfrentar el riesgo y asumirlo.

Recomendaciones

- Debido a la importancia que poseen las tecnologías de la información para apoyar en la consecución de las metas de las organizaciones y además proporcionar beneficios en competitividad, los riesgos que también implica adoptarlas deberían ser tratados como los demás riesgos clave; tal como los riesgos de mercado, de crédito u operativos. Entonces, la mayoría de las decisiones de una organización o empresa requieren que la alta dirección o los gerentes sopesen los riesgos y los beneficios y estas decisiones no sean relegadas a especialistas técnicos debido a que los riesgos de TI no son puramente una cuestión técnica. Indudablemente, se necesitan expertos en la materia para entender y gestionar los aspectos de riesgos de TI, pero el conocimiento sobre la gestión del negocio es lo más importante y por consiguiente los directivos son corresponsables por la gestión de riesgos. Un marco de riesgos como RISK IT permite a las partes interesadas (directivos, gerentes y técnicos) adoptar decisiones apropiadas con conocimiento acerca de la magnitud de los riesgos para deducir cómo

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

responder a los mismos. Por tales motivos, se recomienda aplicar la metodología desarrollada en el presente estudio en instituciones, empresas u organizaciones de cualquier ámbito, tamaño y naturaleza.

- Después de aplicar toda metodología de gestión de riesgos se realiza una etapa de comunicación de riesgos, que implica entender los mismos, expresarlos y discutirlos. Para lo cual, se recomienda que la organización, establezca un plan que implique relacionar a las fuentes y destinatarios de la información sobre riesgos, las formas y canales en que se comunicarán los mismos y la periodicidad con que se realizará este proceso y que todos estos factores, con el tiempo, formen parte de una cultura de riesgos concreta y propia de la organización.

- Cualquier institución, empresa u organización podría ajustar a sus necesidades una metodología, marco o modelo de gestión de riesgos como la concebida en el presente estudio. Un cargo directivo o gerencial, al adoptar una metodología de gestión de riesgos y mantenerla vigente con cierta periodicidad podría beneficiarse de aspectos relacionados con el conocimiento global y específico oportuno sobre los riesgos a los que están expuestos los activos bajo su administración y por consiguiente tener la posibilidad de tomar decisiones de manera consiente e informada. Además, que una metodología de gestión de riesgos como la realizada para el presente trabajo permite mantener actualizado un perfil de riesgos lo que redunda en una adecuada respuesta y una visión clara sobre los eventos que podrían presentarse incluso a futuro. Por tales razones, se recomienda a los cargos gerenciales acompañar e involucrarse en los procesos que implica la adopción y puesta en acción de una gestión de riesgos planificada.

Referencias

Chambi, R. (2018). *Modelo de Gestión de Riesgos de TI bajo COBIT 5*. Repositorio Virtual de Tesis Universidad Mayor de San Andrés

Crespo, P. (Noviembre de 2016). *Metodología de Seguridad de la Información para la Gestión del Riesgo Informático Aplicable a MPYMES*. Repositorio Virtual de Tesis Universidad de Cuenca

Cruces, M., & Mora, J. (Julio de 2016). *Gestión de Riesgo de Seguridad de la Información con Base en la Norma ISO/IEC 27005 de 2011 Adaptando la Metodología COBIT al Caso de Estudio: Procedimiento Recaudos de la División Financiera de la Universidad del Cauca*. Repositorio Virtual de Tesis Universidad del Cauca

Erreyes, D. (2017). *Metodología para la Selección de Herramientas Eficientes y Protocolos Adecuados para Mejorar la Seguridad de los Dispositivos Móviles.* Repositorio Virtual de Tesis Universidad de Cuenca

Gualim, N. (Agosto de 2014). *Plan de Acción para Minimizar la Exposición al Riesgo Tecnológico de una PYME Basada en el Marco de Referencia RISK IT*. Guatemala. Repositorio Vitual de Tesis Universidad San Carlos de Guatemala

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación.* McGraw Hill.

Instituto Nacional de Ciberseguridad. (2017). *INCIBE.* https://www.incibe.es/

ISACA. (2012). *COBIT 5 Marco de Negocio para el Gobierno y Gestión de las TI de la Empresa.*

_____. (2020). Guía Profesional RISK IT. EEUU.

_____. (2020). RISK IT Marco de Riesgos de TI. EEUU.

ISO. (octubre de 2019). *International Organization for Standarization*. Obtenido de https://www.iso.org/home.html

NIST. (2018). *Seguridad Cibernética.* https://www.nist.gov/topics/cybersecurity

RAE. (octubre de 2019). *Real Academia Española*. https://dle.rae.es/?w=riesgo

Yunn, S. (25 de septiembre de 2019). *Introducción a la Seguridad*. Quito, Pichincha, Ecuador.

Cómo citar este artículo:
Arcos, S,. Tapia, F,. Chafla. G. & Nicolade, D. (Julio - diciembre de 2022). Modelo metodológico basado en RISK IT como estrategia para la Gestión de Riesgos Organizacionales. *Sathiri* (17),2 26-46. https://doi.org/10.32645/13906925.1129