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

PLAN DE ACCIÓN PARA MINIMIZAR LA EXPOSICIÓN AL RIESGO TECNOLÓGICO DE UNA PYME BASADA EN EL MARCO DE REFERENCIA RISK IT

Noé Emanuel Gualim Ac

Asesorado por el Ing. Genser Daniel Mayorga Elías

Guatemala, agosto de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PLAN DE ACCIÓN PARA MINIMIZAR LA EXPOSICIÓN AL RIESGO TECNOLÓGICO DE UNA PYME BASADA EN EL MARCO DE REFERENCIA RISK IT

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

NOÉ EMANUEL GUALIM AC
ASESORADO POR EL ING. GENSER DANIEL MAYORGA ELÍAS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO DE 2014

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	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Marlon Antonio Pérez Türk
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADORA	Inga. Virginia Victoria Tala Ayerdi
SECRETARIO	Inga. Marcia Ivónne Véliz Vargas

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:

PLAN DE ACCIÓN PARA MINIMIZAR LA EXPOSICIÓN AL RIESGO TECNOLÓGICO DE UNA PYME BASADA EN EL MARCO DE REFERENCIA RISK IT

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha marzo de 2014.

Noé Emanuel Gualim Ac

Guatemala, 14 de Julio del 2014

Ingeniero
Carlos Azurdia.
Revisor de Tesis
Carrera de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ingeniero:

Por este medio hago de su conocimiento que he revisado el trabajo de investigación titulado *Plan de acción para minimizar la exposición al riesgo tecnológico de una PYME basado en el marco de referencia Risk IT* que el estudiante Noé Emanuel Gualim Ac, quien se identifica con número de carné 199811010, está desarrollando y que hasta la fecha 14 de Julio del 2014 ha completado el trabajo planteado de esta investigación. Manifiesto por este medio mi aprobación por el esfuerzo, dedicación y resultados obtenidos por el estudiante en el desarrollo del trabajo de investigación.

Sin más por el momento y agradeciendo la oportunidad de colaboración a la educación e investigación universitaria que me da, me despido.

Atentamente:

Genser Daniel Mayorga Elías
Ingeniero en Ciencias y Sistemas
No de colegiado. 8149
Asesor

Génser Daniel Mayorga Elias
Ingeniero en Ciencias y Sistemas
Colegiado 8149

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

Guatemala, 23 de Julio de 2014

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 **NOÉ EMANUEL GUALIM AC** con carné **1998-11010,** titulado: **"PLAN DE ACCIÓN PARA MINIMIZAR LA EXPOSICIÓN AL RIESGO TECNOLÓGICO DE UNA PYME BASADA EN EL MARCO DE REFERENCIA RISK IT",** 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, del trabajo de graduación ***"PLAN DE ACCIÓN PARA MINIMIZAR LA EXPOSICIÓN AL RIESGO TECNOLÓGICO DE UNA PYME BASADA EN EL MARCO DE REFERENCIA RISK IT"****, realizado por el estudiante NOÉ EMANUEL GUALIM AC, 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 Türk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 26 de agosto 2014

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.D.425-2014

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: **PLAN DE ACCIÓN PARA MINIMIZAR LA EXPOSICIÓN AL RIESGO TECNOLÓGICO DE UNA PYME BASADA EN EL MARCO DE REFERENCIA RISK IT,** presentado por el estudiante universitario: **Noé Emanuel Gualim Ac** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, agosto de 2014

/cc

ACTO QUE DEDICO A:

Dios Por darme la oportunidad de alcanzar mis sueños, iluminar mi camino y darme la fortaleza necesaria para continuar en los momentos más difíciles de mi vida.

Mis padres Arcelia Ac de Gualim y Miguel Gualim. Por el gran amor que me han dado, sus enseñanzas de vida y el esfuerzo realizado para formarme como una persona de bien.

Mi esposa Jessica Valdizón. Por ser el motor que me impulsó a alcanzar este sueño y por ser el complemento de mi vida que en todo momento me brinda su apoyo incondicional. Te amo mi cielo.

Mis tías Virginia Ac, por siempre estar al lado de nuestra familia apoyándonos incondicionalmente y ser una madre más. Armenia Ac (q.e.p.d.) y Concepción Gualim (q.e.p.d.) por sus valiosos consejos y cariño.

Mis hermanos y hermanas	Miguel, Juan, Migdalia y Andrea Gualim Ac, por estar siempre apoyándome y ser parte fundamental del esfuerzo para alcanzar este sueño.
Mis sobrinos	Por ser una bendición y alegría para mi vida.
Mi primo	Mario Ac, por ser un hermano más y por el gran apoyo brindado cuando más lo necesite.

AGRADECIMIENTOS A:

La Universidad de San Carlos de Guatemala	Por ser la casa de estudios que me abrió las puertas para mi preparación académica.
Facultad de Ingeniería	Por la enseñanza brindada para forjarme como un profesional.
Mis amigos de la Facultad	Ing. Danilo Ac, Ing. Víctor Castillo, Miguel Divas, Ing. Eddy Guaran y Viviana Vaides con especial aprecio.
Mi asesor	Ing. Genser Daniel Mayorga, por su apoyo incondicional.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES V
GLOSARIO VII
RESUMEN XVII
OBJETIVOS XIX
INTRODUCCIÓN XXI

1. MARCO TEÓRICO 1
1.1. Riesgo 2
1.2. Riesgo tecnológico 2
1.2.1. Clasificación del riesgo tecnológico 4
1.2.2. Origen del riesgo tecnológico 6
1.2.3. Escenarios de riesgo 8
1.2.4. Impacto del riesgo tecnológico 10
1.3. Gestión del riesgo tecnológico 13
1.3.1. Identificación de riesgos 14
1.3.2. Análisis o evaluación de riesgos 15
1.3.3. Priorización de riesgos 16
1.3.4. Mitigación de riesgos 17
1.3.5. Monitoreo y control de riesgos 17
1.3.6. Cultura del riesgo 18
1.4. Marco de referencia Risk IT 20
1.4.1. Estructura Risk IT 22
1.4.1.1. Gobierno de riesgos (GR) 23
1.4.1.2. Evaluación de riesgos (ER) 24
1.4.1.3. Respuesta de riesgos (RR) 25

1.4.2. Público y partes interesadas al que se dirige Risk IT 26
1.4.3. Principios del riesgo de TI 29
1.4.4. Fundamentos de la evaluación del riesgo de TI 30
1.4.5. Fundamentos de la respuesta de riesgo 32
1.4.6. Beneficios de implementar Risk IT 36

2. NIVEL DE MADUREZ DE UNA PYME EN LA GESTIÓN DEL RIESGO TECNOLÓGICO 39
2.1. Nivel de madurez 39
2.2. Metodología para determinar el nivel de madurez 46
2.3. Criterios para determinar el nivel de madurez 49
2.3.1. Manejo e implementación de estándares 49
2.3.2. Dominios del Framework Risk IT 50
2.3.3. Procesos del Framework Risk IT 51
2.3.4. Actividades gestión de riesgos Framework Risk IT 52
2.3.5. Categorías generales gestión de riesgos de TI 57

3. EVALUACIÓN DEL NIVEL DE MADUREZ DE UNA PYME 59
3.1. Definición de encuesta 59
3.2. Interpretación de resultados 60
3.2.1. Aspectos generales de evaluación de riesgos 60
3.2.2. Aplicación de estándares para la gestión de riesgos tecnológicos 61
3.2.3. Ejecución de procesos de gestión de riesgos tecnológicos según Risk IT 64
3.2.4. Cumplimiento de dimensiones de gestión de riesgos tecnológicos según Risk IT 68

3.2.5. Cumplimiento de criterios generales de administración de riesgos 69
3.3. Nivel de madurez en la gestión de riesgos de TI 71
3.3.1. Nivel de madurez gobierno de riesgos de TI 72
3.3.2. Nivel de madurez evaluación de riesgos de TI 73
3.3.3. Nivel de madurez respuesta a riesgos de TI 74

4. PLAN DE ACCIÓN PARA MINIMIZAR EL RIESGO TECNOLÓGICO BASADO EN RISK IT 77
4.1. Organización de la gestión de riesgos 78
4.1.1. Alinear la estrategia del negocio a los objetivos de TI 78
4.1.2. Evaluar la capacidad de TI 79
4.1.3. Definir el nivel de madurez deseado 80
4.1.4. Definir roles y responsabilidades para la gestión de riesgos 80
4.1.5. Identificar del las principales líneas del negocio y procesos prioritarios 82
4.2. Definición de políticas, procedimientos y normas de gestión de riesgos 82
4.2.1. Política de gestión de riesgos 83
4.2.2. Procedimientos para la gestión de riesgos 85
4.2.3. Normas para la gestión de riesgos 86
4.3. Fomentar la gestión de riesgos 86
4.4. Implementación del modelo de gestión de riesgos 87
4.4.1. Definición del alcance de la gestión de riesgos 88
4.4.2. Definición de criterios de evaluación, impacto y aceptación de riesgos 89
4.4.2.1. Criterios para la evaluación de riesgos .. 90

4.4.2.2. Criterios para determinar el impacto.....90
4.4.2.3. Criterios para la aceptación de riesgos ..91
4.4.3. Identificación y documentación de riesgos.....91
4.4.3.1. Identificación de activos 92
4.4.3.2. Identificación de amenazas.....93
4.4.3.3. Identificación de vulnerabilidades.....94
4.4.4. Evaluación y medición de riesgos 95
4.4.4.1. Determinación de la frecuencia 97
4.4.4.2. Determinación del impacto 98
4.4.4.3. Ponderación de factores de riesgo 99
4.4.4.4. Análisis de controles.....100
4.4.4.5. Determinar el riesgo residual y niveles de tolerancia.....102
4.4.5. Priorización y definición de respuesta al riesgo.....103
4.4.6. Plan de tratamiento del riesgo.....104
4.4.7. Monitoreo 104
4.5. Definición de procedimiento de gestión de riesgos 105
4.6. Gestión de comunicación.....107
4.7. Seguimiento y supervisión de la gestión de riesgos.....108
4.8. Mejora continua.....110
4.9. Actividades para mitigar el riesgo tecnológico 110

CONCLUSIONES.....113
RECOMENDACIONES 115
BIBLIOGRAFÍA.....117
APÉNDICE 123
ANEXOS.....149

ÍNDICE DE ILUSTRACIONES

FIGURAS

1. Árbol de confiabilidad de sistemas de información 1
2. Categoría de los riesgos de TI 5
3. Fuentes de riesgos 7
4. Componentes del escenario de riesgo 9
5. Gestión de riesgos: entradas y salidas 14
6. Elementos de la cultura de riesgos 19
7. Marco de riesgos de TI 22
8. Modelo de madurez 40
9. Proceso evaluación modelo de madurez 48
10. Frecuencia de aplicación de estándares para la gestión de riesgos de TI 62
11. Frecuencia de ejecución de actividades de los procesos del Framework Risk IT 64
12. Frecuencia de ejecución de actividades de los dominios del Framework Risk IT 68
13. Aplicación de criterios generales para la gestión de riesgos 70
14. Procedimiento gestión de riesgos tecnológicos 106

TABLAS

I. Mapa de riesgos según su impacto y probabilidad de ocurrencia 16
II. Niveles para medir la frecuencia de ejecución de actividades de la gestión de riesgos 47

III. Dimensiones de implementación de estándares 49
IV. Dominios del Framework Risk IT para evaluar el nivel de madurez 50
V. Procesos del Framework Risk IT para evaluar el nivel de madurez 51
VI. Actividades del Framework Risk IT para evaluar el nivel de madurez 53
VII. Categorías para evaluar la gestión de riesgos de TI..... 57
VIII. Matriz de trabajo de escenarios de riesgo 96
IX. Clasificación de probabilidad de ocurrencia de un riesgo 97
X. Clasificación de impacto por materialización de amenazas 99
XI. Clasificación nivel de exposición de riesgos 100
XII. Niveles de tolerancia de riesgos 103
XIII. Ponderación eficacia de controles de riesgos..... 109
XIV. Actividades sugeridas para mitigar el riesgo..... 110

GLOSARIO

Amenaza Es la probabilidad de ocurrencia de cualquier tipo de evento o acción que pueda generar daño ya sea material o inmaterial sobre algún elemento, poniéndolo en peligro y pudiendo desencadenar eventos de pérdida.

Apetito al riesgo Es la cantidad de riesgo que una organización está dispuesta a aceptar en el cumplimiento de su misión o visión. Este depende de la capacidad objetiva de la organización para absorber pérdidas y, la cultura o predisposición a asumir riesgos prudentes o agresivos para alcanzar sus objetivos estratégicos.

Ataque Es una amenaza que se convierte en realidad ya que llega a ejecutarse, sin importar si esta tuvo éxito o no.

Autenticidad Se refiere a la legitimidad y credibilidad comprobada de una persona, servicio o elemento.

BCP	Plan de Continuidad del Negocio (por sus siglas en inglés Business Continuity Planning), son los planes logísticos o acciones a seguir por una organización para recuperar y/o restaurar sus funciones críticas dentro de un tiempo determinado, que han sido parcial o totalmente interrumpidas por la materialización de un riesgo no deseado o un desastre.
BSC	Balanced Scorecard, es una herramienta de gestión que traduce la estrategia de la empresa en un conjunto coherente de indicadores que miden el desempeño y cumplimiento de acciones puntuales definidas para alcanzar la estrategia de la empresa desde cuatro perspectivas: 1) financiera, 2) clientes, 3) procesos internos y formación, y 4) crecimiento.
CIO	Chief Information Officer, es el responsable de proveer una visión tecnológica y liderazgo para desarrollar e implementar iniciativas de IT capaces de mantener a la empresa en una posición de liderazgo dentro de un mercado altamente competitivo y cambiante.

COBIT	Modelo para el gobierno de TI desarrollado por ISACA; normativa que proporciona un marco integral que ayuda a las organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectiva de los recursos y servicios de TI de la organización.
Control	Se refiere a las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar que los objetivos del negocio sean alcanzados y que los riesgos identificados sean prevenidos, detectados o corregidos de tal forma que se pueda minimizar el impacto si estos llegaran a materializarse.
Control defectivo	Controles diseñados para descubrir eventos, irregularidades o resultados no previstos. Alertan la presencia de riesgos para tomar medidas inmediatas.
COSO	Committee of Sponsoring Organizations, Comité de Organizaciones Patrocinadoras de la Comisión Treadway quienes definieron un marco de trabajo que describe los componentes necesarios para la gestión de riesgos empresariales.

COTS	Commercial off-the-shelf. Se refiere a un componente tomado fuera del estante. Termino del Reglamento Federal de Adquisiciones (FAR) que define un elemento no-desarrollativo (NDI) de suministro, que es a la vez comercial y se vende en grandes cantidades en el mercado comercial.
Disponibilidad	Garantía de acceso a la información en el momento oportuno y necesario.
DRP	Disaster Recovery Plan. Es un plan de recuperación ante desastres; proceso de recuperación que cubre los datos, hardware y software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.
Elementos de información	Corresponde a aquellos componentes que almacenan o mantienen información de una organización y pueden clasificarse en: a) datos de información, b) sistemas e infraestructura y, c) personal.
ERM	Acrónimo de Enterprise Risk Management (Gestión de riesgos empresariales o corporativos).

ERP	Acrónimo de Enterprise Resource Planning. Es un Software de gestión integrada que permite planificar recursos empresariales y administrar los procesos operativos de las empresas.
Evento de pérdida	Se refiere a la generación o materialización en un lugar y tiempo particular de los eventos que producen efectos negativos para la organización.
Gestión del riesgo	Consiste en el método para determinar, analizar, valorar y clasificar el riesgo al cual se encuentra expuesta una organización, con el fin de implementar mecanismos que permitan controlar y mantener los riesgos en un nivel tolerable. La gestión de riesgos se encuentra formada por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de riesgos.
Impacto	Magnitud que mide el número de repeticiones por unidad de tiempo de cualquier fenómeno, escenario, acontecimiento o suceso periódico.
Indicador	Definición de datos que ayudan a medir objetivamente la evolución de una actividad o una tarea, así como la efectividad y desempeño de un control establecido para mitigar un riesgo.

Integridad	Garantía de que los datos son completos y válidos; que todos los cambios a los datos son reproducibles permitiendo saber el responsable del cambio y el momento del cambio.
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.
KRI	Acrónimo de Key Risk Indicator. Un indicador de riesgos clave es una métrica para determinar qué tan posible es que la probabilidad de un evento combinada con sus consecuencias, supere el apetito de riesgo de la organización (es decir, nivel de riesgo que la compañía está dispuesta a aceptar), y tenga un impacto negativo sobre la capacidad de tener éxito de una organización.
Medición	Proceso mediante el cual se compara un patrón seleccionado con el objeto o fenómeno cuya magnitud física se desea medir para determinar cuántas veces el patrón está contenido en esa magnitud.

Metodología	Conjunto de procedimientos racionales utilizados para alcanzar objetivos que rigen una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Alternativamente puede definirse la metodología como el estudio o elección de un método pertinente para un determinado objetivo.
Monitoreo	Control o supervisión de un escenario específico sobre el cual se desea conocer el comportamiento para reaccionar o dar respuestas si se llegara a dar fuera de los límites o parámetros establecidos.
Norma	Regla o conjunto de reglas que deben seguirse para llevar a cabo una acción, para obtener un resultado esperado y controlado.
Propensión al riesgo	También conocida como apetito al riesgo, es el nivel de riesgo máximo que una empresa está dispuesta a aceptar para lograr sus objetivos.
RACI	Matriz de asignación de responsabilidades la cual es utilizada para relacionar actividades con recursos que pueden ser individuos o equipos de trabajo. Los roles que refleja esta matriz son Responsible (Responsable), Accountable (Aprobador), Consulted (Consultado) e Informed (Informado), en esta matriz, se asigna el rol que el recurso debe jugar para cada actividad dada.

Riesgo Según el Diccionario de la Real Academia Española[1], la palabra riesgo viene del árabe *rizq* (lo que depara la providencia) a través del italiano *rischio*. Riesgo, se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas[2]; el riesgo se encuentra vinculado a la vulnerabilidad y amenaza.

Riesgo inherente Es el riesgo de que ocurran errores importantes generados por las características de la empresa o el organismo.

Riesgo operacional Riesgo que puede generar pérdidas directas o indirectas cuyo origen corresponde a errores humanos, procesos internos inadecuados o defectuosos, controles internos inadecuados, fallas en los sistemas o por acontecimientos externos originados dentro de la propia operación de una empresa.

Riesgo residual Riesgo asociado a un evento después de implementado un control que se encuentre en ejecución con el fin de mitigar dicho riesgo.

---

[1] *Diccionario de la Real Academia Española* – 22ª Edición – 2001.

[2] UNISDR, *Terminología sobre reducción de riesgo de desastres 2009 para los conceptos de amenaza, vulnerabilidad y riesgo*.

Risk IT	Marco basado en guías, principios, procesos de negocio y directrices de gestión implementadas para la gestión eficaz de los riesgos de TI; establece mejores prácticas con el fin de proporcionar a las empresas un marco de referencia para identificar, gobernar y administrar los riesgos tecnológicos asociados a su negocio, logrando con esto una mejor gestión de riesgos de TI dentro de la organización.
Seguridad informática	Corresponde a las actividades, procesos y mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.
Severidad	Asociado a riesgos, es el valor asignado al daño más probable que produciría si se materializa un riesgo. La severidad de un riesgo se puede clasificar como baja (daños superficiales o pérdidas leves), media (perdidas graves) o alta (pérdida de material muy grave).
SIB	Superintendencia de Bancos, entidad responsable de promover estabilidad y confianza en el sistema financiero supervisado de Guatemala.
TI	Acrónimo de Tecnologías de la Información.

Tolerancia	Se refiere a la acción y efecto de tolerar o aceptar un riesgo al cual se encuentra expuesta una empresa. La tolerancia de riesgos se define a nivel de organización y se refleja en las políticas; el apetito de riesgo establecido no debe ser superado por la exposición total al riesgo.
Val IT	Framework de gobernabilidad que apoya a la creación de valor de negocio de las inversiones en TI. Consiste en un conjunto de principios rectores y una serie de procesos y mejores prácticas definidos como un conjunto de prácticas de gestión claves para apoyar y ayudar a la gerencia ejecutiva a nivel empresarial.
Vulnerabilidad	Condiciones, características y capacidad de un sistema que lo hacen susceptible a amenazas y, como resultado se ven expuestas a sufrir algún daño. Corresponde a los acontecimientos que contribuyen a la magnitud o frecuencia de eventos de pérdida que ocurren.
WAN	Wide Area Network. Red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas.

RESUMEN

En la actualidad las empresas buscan dar a sus clientes una propuesta de valor que satisfaga sus necesidades y que a su vez les permita maximizar las utilidades, minimizar los costos y optimizar el uso de sus recursos; para lograrlo se apoyan en el uso de tecnología para ejecutar sus operaciones, lo cual hace que las PYMES, requieran soportar su crecimiento y competir a nivel global adoptando nuevas tecnologías de manera ágil y flexible.

Mientras una organización dependa más de la tecnología para gestionar sus operaciones, se incrementa la exposición al riesgo relacionado a factores tecnológicos; por lo cual, es necesario que los responsables de tecnología tenga claros los riesgos a los cuales su empresa se encuentra expuesta y en conjunto con la dirección del negocio y el comité ejecutivo, establezcan los mecanismos para mitigar el riesgo y llevarlo hasta umbrales de tolerancia de acuerdo al apetito al riesgo que estén dispuestos a asumir.

En Guatemala existen iniciativas para regular la gestión del riesgo tecnológico sin embargo, estas se enfocan en entidades financieras como lo es la SIB que se encarga de velar por el cumplimiento de las resoluciones emitidas por la Junta Monetaria JM-056-2011 y JM-102-2011, no cubriendo empresas que no pertenecen al sector financiero. El presente trabajo consiste en evaluar el nivel de madurez de una PYME en la gestión de riesgos y establecer un plan de acción para minimizar la exposición al riesgo tecnológico, definiendo actividades de gestión, análisis y respuesta a riesgos como parte de un proceso cíclico tomando como base el Framework Risk IT.

OBJETIVOS

General

Proveer un plan de acción para minimizar la exposición al riesgo tecnológico en una PYME basada en Risk IT.

Específicos

1. Dar a conocer los conceptos relacionados a la gestión de riesgos de TI.

2. Conocer la importancia de la gestión del riesgo tecnológico y su impacto en el negocio.

3. Aplicar el marco de referencia Risk IT para determinar la situación actual de la gestión de riesgos tecnológicos en una PYME.

4. Determinar el nivel de madurez de una PYME para la gestión de riesgos tecnológicos.

5. Establecer las acciones para minimizar el riesgo por medio de un plan de acción que permita identificar los riesgos a los que se encuentra expuesta una PYME.

INTRODUCCIÓN

Hoy en día una fuente fundamental para las organizaciones de mantenerse a la vanguardia es implementar cambios radicales que les permitan optimizar sus procesos, mejorar sus servicios, tener control sobre su información y, satisfacer las necesidades de sus clientes ofreciéndoles propuestas de valor que llenen las expectativas de los segmentos a los cuales se encuentra orientado su modelo de negocio.

Para lograr estos objetivos, las organizaciones deben implementar ideas innovadoras que en su mayoría se enfocan en apoyarse en la implementación de tecnología, sistemas de información, infraestructura y herramientas tecnológicas que, si bien es cierto, generan un valor agregado a su gestión y mejores resultados, las expone a riesgos tecnológicos; mientras más dependientes se encuentren de TI mayor es la exposición a riesgos de TI, que al llegar a materializarse pueden llegar a representar considerables pérdidas para la organización, impactando a nivel económico, imagen o credibilidad.

Con el afán de mitigar este tipo de riesgo, la comunidad informática y otros profesionales en la materia se han enfocado en incorporar a normativas de mejores prácticas la gestión del riesgo tecnológico, adaptando los modelos y reestructurando sus procesos así como incorporando el conocimiento adquirido en la preparación de la normativa como ISO 31000, adaptaciones realizadas al marco ITIL o la creación de certificaciones como CRISK por parte de ISACA, cuya organización internacional se dedica al control del gobierno corporativo mediante la implementación de mejores prácticas como COBIT y el marco de referencia Risk IT.

Considerando que el riesgo tecnológico no solo corresponde a aquel al que una entidad se encuentra expuesta por mala fe o dolo de una persona o entidad, sino que también es aquel que se origina de manera directa por falla o alteración del funcionamiento de infraestructura, sistemas de información y procesos, asimismo, es aquel que se genera de manera indirecta por situaciones externas que se escapan del control de las entidades pudiendo ser desastres naturales o accidentes que al llegar a materializarse pueden ocasionar la suspensión de servicios e interrumpir el funcionamiento normal.

Tal y como se manifiesta en el informe de Verizon correspondiente a la investigación de brechas en los datos de 2014, donde se manifiesta que "la seguridad de los datos debe importarle sea cual sea su papel en la organización[3]", es importante gestionar el riesgo considerando que las consecuencias económicas pueden ser enormes ya que al materializarse un riesgo tecnológico, puede impactar de forma considerable sobre aspectos relacionados con el deterioro de la imagen de la empresa, medio ambiente y aspectos legales que pueden derivar en sanciones o daños punitivos y, ocasionar costos significativos y extraordinarios para las empresas que afecten de forma negativa sus operaciones.

El presente trabajo muestra el enfoque de análisis de riesgos basado en Risk IT identificando las consideraciones mínimas que debiera tener una PYME para implementar procesos, controles y acciones para gestionar el riesgo tecnológico; asimismo, proporciona una guía que permite establecer el nivel de madurez en la gestión de riesgos de TI sobre los tres dominios sobre los cuales se enfoca el marco de referencia Risk IT.

[3] Verizon. *Resumen ejecutivo informe sobre investigación de brechas en los datos de 2014*, p. 2

Se presenta una base conceptual de la gestión de riesgos de TI los cuales son aquellos que se encuentran relacionados al uso de la tecnología dentro de una empresa para poder gestionar sus operaciones, también introduce al lector al Framework Risk IT sobre el cual se basa este trabajo.

Se establecen los criterios para medir el nivel de madurez en la gestión de riesgos tecnológicos en una PYME basándose en tres perspectivas, la primera consiste en evaluar el cumplimiento de estándares, la segunda en criterios generales de gestión de riesgos y por último el nivel de madurez basado en los dominios definidos por el Framework Risk IT los cuales comprenden el gobierno de riesgos, la evaluación de riesgos y la respuesta a riesgos.

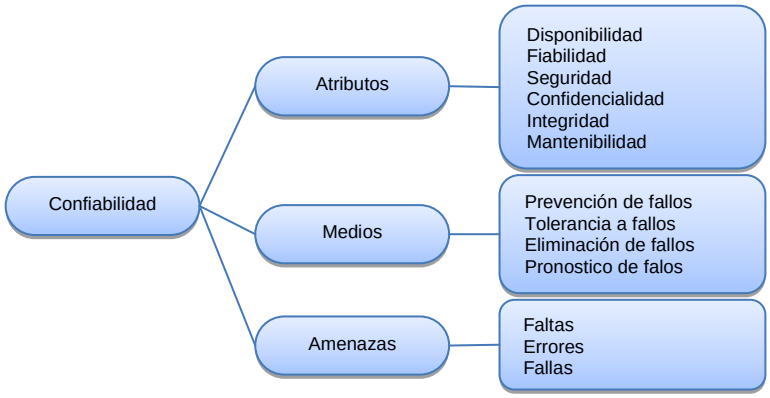
Se determina el nivel de madurez en la gestión de riesgos de la PYME analizada, en donde llegamos a materializar la evaluación definiendo los aspectos a evaluar por medio de una encuesta que se basa en las actividades definidas en el Framework de Risk IT, cuyos resultados son trasladados a gráficos de tela de araña para determinar la frecuencia con que se realizan las actividades evaluadas e interpretar los resultados.

Se determina el plan de acción que debe seguir la PYME evaluada para minimizar la exposición al riesgo tecnológico proveyendo una metodología de análisis de riesgos y las prácticas a realizar para gestionar el riesgo, evaluarlo y dar respuesta al mismo, permitiendo identificar los riesgos a los cuales se encuentra expuesta la organización, medir el nivel de exposición, niveles de tolerancia y bases para gestionar, controlar y mitigar el riesgo tecnológico.

1. MARCO TEÓRICO

La confianza que obtienen los usuarios tanto internos como externos, depende de cómo perciben el comportamiento del servicio que reciben mediante sistemas informáticos. La confiabilidad según Algirdas Avizienis en el documento Fundamental Concepts of Dependability, se define como "la propiedad de un sistema informático que nos permite tener justificadamente confianza sobre el servicio que proporciona". Asimismo indica que todo sistema informático posee cuatro características fundamentales: funcionalidad, rendimiento, costo y confiabilidad, donde la confiabilidad presenta una exposición sistemática dada por amenazas, atributos y medios, ver figura 1.

Figura 1. **Árbol de confiabilidad de sistemas de información**



Fuente: Fundamental Concepts of Dependability, Research Report N01145, LAAS-CNRS.

Un sistema es confiable si se encuentra disponible, preparado para el uso en cualquier momento, si es fiable presentando continuidad de servicio, si se

encuentra fuera de peligro evitando consecuencias catastróficas y si es seguro previniendo accesos y teniendo el control de información no autorizada.

1.1. Riesgo

Según el Diccionario de la Real Academia Española[4], la palabra riesgo proviene del árabe *rizq* (lo que depara la providencia) a través del italiano *rischio*. El riesgo, es la exposición que se tiene a la probabilidad de ocurrencia de eventos y consecuencias negativas, como pérdida económica, daño físico, retrasos, pérdida de información, entre otros.

El concepto riesgo se compone de dos elementos: la probabilidad de ocurrencia y las consecuencias si estas llegaran a ocurrir (impacto o severidad); donde la probabilidad de ocurrencia se ve influenciada por la existencia de eventos voluntarios o involuntarios que al llegar a materializarse generan consecuencias negativas pudiendo afectar de forma parcial e incluso total paralizando operaciones, lo cual dependerá del impacto y nivel de tolerancia que se presente ante tal exposición.

1.2. Riesgo tecnológico

Existen diferentes tipos de riesgos a los cuales una organización se encuentra expuesta, como por ejemplo el riesgo operacional, riesgo de mercado, riesgos ambientales, riesgos financieros, riesgos estratégicos, riesgos de cumplimiento, entre otros.

[4] *Diccionario de la Real Academia Española* – 22ª Edición – 2001.

El riesgo tecnológico es uno de los riesgos a los cuales se encuentra expuesta una organización cuando esta depende de la tecnología para realizar sus operaciones, debido a esto, con los cambios constantes y evoluciones de la tecnología, el nivel de exposición se incrementa para las organizaciones afectando diferentes áreas y, exponiendo el cumplimiento de la propuesta de valor, cumplimiento de objetivos estratégicos, acuerdos de servicio y correcta operación de la organización, entre otros.

Un riesgo tecnológico es considerado como un riesgo operativo ya que el desarrollo de una organización se encuentra dependiente de la tecnología, asimismo, un riesgo tecnológico, es un riesgo del negocio, el cual se encuentra asociados al uso, propiedad, operación, participación, influencia y adopción de tecnología en una organización; se componen de eventos relacionados a la tecnología que potencialmente pueden afectar al negocio. Este hecho puede ocurrir con una frecuencia y magnitud incierta, y supone que genera dificultades a la misma organización para alcanzar sus metas y objetivos estratégicos, por lo tanto genera cierta influencia para obtener los resultados esperados.

En resumen, un riesgo tecnológico es todo evento, falla o bien, que pone en peligro la integridad, confidencialidad o la disponibilidad de la información o los recursos y activos de una organización, limitando su operación y afectando sus resultados. Asimismo, es aquel que ocasiona pérdidas por la interrupción, falla o daño derivadas de los sistemas de información y plataformas tecnológicas utilizadas por una organización para operar y así poder brindar sus servicios ordinarios.

1.2.1. Clasificación del riesgo tecnológico

El riesgo tecnológico, puede clasificarse de diferentes maneras, cuya clasificación según el marco de riesgos de IT es:

- Riesgo en la realización de beneficios o valor de TI: son los riesgos asociados al no aprovechamiento de oportunidades que brinda el uso de la tecnología para mejorar la eficiencia o efectividad de los procesos del negocio, o el no utilizarlos como facilitadores o habilitadores de nuevas iniciativas de negocio.

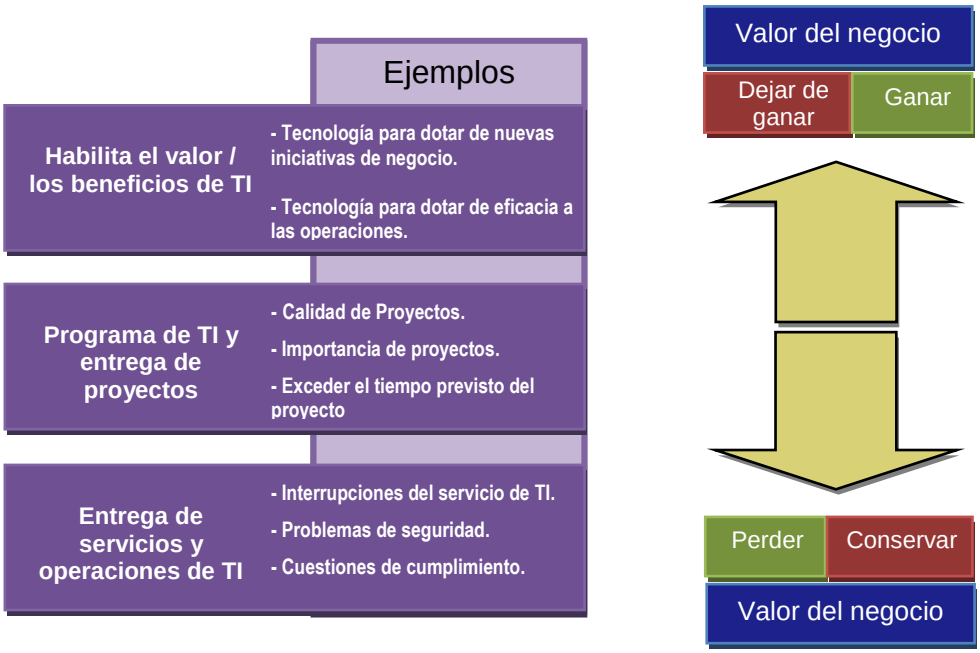
- Riesgo en la entrega de soluciones de TI: el cual se encuentra asociado a la contribución de las TI para soluciones de nuevos negocios o mejoras que por lo general se presentan en la forma de proyectos y programas; se encuentran directamente relacionadas a la planeación estratégica de una organización y se vincula a las inversiones de cartera.

- Riesgo en la entrega de servicios de TI: estos se encuentran asociados con todos los aspectos de desempeño de TI y los servicios de sistemas que puedan llegar a ocasionar perdidas o la reducción de valor para la organización; son presentados por medio de servicios para garantizar la operación de la organización.

Los riesgos de TI existen sin importar si estos son o no detectados o identificados por la organización; la figura 2 muestra que para cada una de las categorías definidas para los riesgos de TI, existe un aspecto positivo equivalente con lo cual las organizaciones al ocupar parte de sus recursos a la gestión del riesgo tecnológico, pueden obtener resultados positivos que les

beneficien, por lo cual, es indispensable mantener una relación riesgo/beneficio al momento de tomar una decisión para gestionar el riesgo.

Figura 2. **Categoría de los riesgos de TI**



Fuente: Framework Risk IT, ISACA.

La gestión de riesgos, deberá cubrir los siguientes riesgos de TI:

- Seguridad y accesos: riesgo de acceso y uso de información confidencial por personas no autorizadas.

- Integridad: riesgo que la información no sea confiable, se presente incompleta e inexacta.

- Pertinente: riesgo de no contar con la información adecuada en el tiempo preciso para el proceso.

- Disponibilidad: riesgo de pérdida de servicios.

- Infraestructura: riesgo de no contar con la infraestructura acorde a las necesidades actuales y futuras del negocio.

1.2.2. Origen del riesgo tecnológico

Considerando que los riesgos que se encuentran asociados a la tecnología, desde su concepción, desarrollo y utilización, los cuales no solo impactan a las organizaciones que las conciben durante su periodo de desarrollo; los orígenes pueden ser diversos, de los cuales, los más frecuentes según Antonio Hidalgo Nuchera, son:

- Derivado del proceso de adquisición o transferencia de tecnología: regularmente, estos son ocasionados por razones internas originadas de planificaciones deficientes o son ocasionados por la falta de adaptación de los recursos humanos que se encuentran implicados en el proceso.

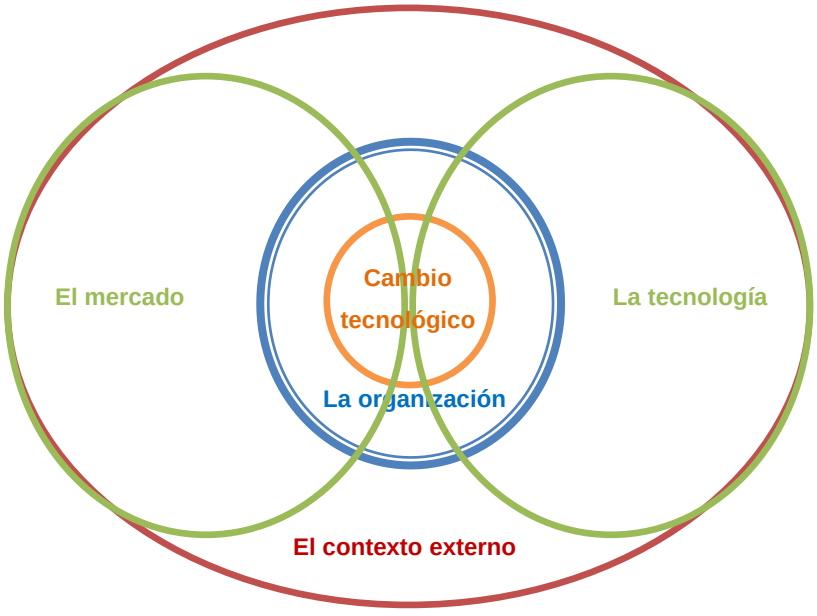
- Originados por dificultades en la organización receptora: son causas que tienen su origen en la organización que dará uso a la TI y que afectan el desarrollo o implantación.

- Derivadas de la tecnología utilizada para su desarrollo: regularmente son originados por el uso de una tecnología inestable o que se vuelve obsoleta.

- Derivadas de factores externos a la organización: corresponden a factores fuera del alcance de la organización que imposibilitan el acceso a la tecnología, su mantenimiento o soporte para continuar con su uso, cuyos factores pueden estar relacionados a causas socioeconómicas o políticas, entre otras.

- Derivadas del mercado y su evolución durante el desarrollo de la tecnología: se encuentran relacionadas a acontecimientos no previstos que pueden impactar directamente en los resultados esperados durante el desarrollo de la tecnología; se encuentran relacionados a aspectos económicos y de penetración tecnológica que a pesar de no estar ligados a las TI, les impacta desfavorablemente, como por ejemplo, una crisis económica global, recesión económica y caídas del valor del dinero.

Figura 3. **Fuentes de riesgos**



Fuente: *Introducción a la gestión de riesgos tecnológicos*, Universidad Politécnica de Madrid.

Los orígenes del riesgo tecnológico no son únicos y estos muchas veces se encuentran relacionados entre sí, por lo cual es importante que al momento de realizar un análisis de riesgos se realice de forma diferente para cada escenario, evaluando el entorno aplicable para el caso estudiado. La figura 3, muestra la relación entre los diferentes orígenes del riesgo tecnológico que como se podrá observar, se encuentran relacionados, sin embargo no en todos los casos se presenta esta situación.

Dado que se tienen múltiples orígenes de riesgo y estos pueden presentarse en diferentes circunstancias, generando escenarios diferentes acorde a eventos que se presenten en el momento en que se genera el riesgo o se llega a concebir, los posibles eventos relacionados a un riesgo pueden estar sujetos a fraudes internos, fraudes externos, clientes, productos y servicios, daños físicos, interrupción de negocios e incluso la administración de procesos.

1.2.3. Escenarios de riesgo

Un escenario de riesgo es la descripción o explicación de un evento relacionado con TI que representa un riesgo para el negocio, de acuerdo al marco de trabajo de riesgos de IT, de ISACA, para que los escenarios de riesgo sean completos, deben contar con elementos o factores de riesgo.

La estructura del escenario de riesgos difiere de acuerdo al evento de pérdida, vulnerabilidad y amenaza; para que un riesgo se materialice y a su vez para que estos puedan analizarse por medio de simulaciones de los mismos, deben contar con todos los elementos que se muestran en la figura 4.

Figura 4. **Componentes del escenario de riesgo**

Fuente: Framework Risk IT, ISACA.

Los componentes del escenario de riesgo, se describen a continuación:

- Actor: es quien genera la amenaza el cual puede ser interno o externo y puede ser o no, una persona.

- Tipo de amenaza: corresponde al tipo de evento o clasificación con la cual puede definirse su naturaleza; esta puede ser ocasionada de forma accidental o malintencionada, falla de un proceso ya sea por no cumplirlo o porque no se tiene contemplado el evento, o bien puede ser ocasionado por un evento natural fuera del alcance de la empresa.

- Acción: es el evento que se genera por la materialización u ocurrencia del riesgo sobre un activo de la organización generando un impacto en el negocio.

- Activo: es un recurso que ayuda a lograr los objetivos de TI pudiendo ser las personas, la organización, los procesos, la infraestructura física, infraestructura de TI o, componentes de la arquitectura de la organización (información y aplicaciones), cada uno de los activos o recursos dentro de la organización deberá ser catalogado por su criticidad por lo cual para la gestión de riesgos, deberá priorizarse aquellos activos con mayor impacto y criticidad para la empresa.

- Tiempo: componente que denota la periodicidad y duración del escenario de riesgo al momento de que este se materialice, asimismo, dependiendo del momento en que se materialice puede llegar a ser considerable o no; por ejemplo, si se genera en un momento crítico y si este genera una consecuencia inmediata que impacte directamente en la operación de la empresa o su impacto sea retardado que no es perceptible para los usuarios.

1.2.4. Impacto del riesgo tecnológico

Durante muchos años el impacto del riesgo tecnológico fue asociado solamente a las áreas de tecnología siendo estas los responsables de cada uno de los incidentes que ocurrían si en algún momento se llegaban a materializar los escenarios de riesgo, es por ello que la evaluación de riesgos de TI, así como las decisiones que se tomen para su mitigación, deben ser expresadas en términos del negocio de tal forma que estos sean comprensibles por las diferentes partes involucradas (áreas de tecnología y áreas del negocio);

debiendo poder comprender y expresar cada una de las áreas del negocio, cómo se ve impactada la empresa si algún riesgo se materializa, generando eventos adversos que impactan a los objetivos estratégicos de la empresa.

Por lo tanto una persona del negocio debe entender como fallos o eventos relacionados a TI pueden llegar a impactar en el negocio, afectando los procesos y servicios claves, asimismo, una persona de TI debe comprender como fallos o eventos relacionados a TI pueden ocasionar pérdidas de forma directa o indirecta en la organización, afectando los objetivos estratégicos.

La forma de describir el impacto que presenta el riesgo tecnológico al negocio, dicho de otra forma, traducir el riesgo tecnológico expresado en términos del negocio, puede realizarse siguiendo diferentes métodos de los cuales se deberá seleccionar alguno, sin embargo, se sugiere aplicar los criterios de Información COBIT; en la guía profesional de riesgos de TI de ISACA, se describe como aplicar los siguientes métodos:

- Criterios de información COBIT: se enfoca en expresar los riesgos de TI en aspectos comerciales, basándose en que el impacto se encuentra en no contar con la información, siendo una descripción intermedia y no una definición del impacto del negocio. Esta se concentra en definir el impacto a través de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, conformidad y cumplimiento.

- Criterios de Balanced Scorecard – BSC: se enfoca en los objetivos del negocio desde las perspectivas financieras, del cliente, internas y de crecimiento.

- Criterios extendidos BSC: la lógica es similar a la anterior, sin embargo, esta se concentra en bajar a un nivel más especifico en donde se consideran los aspectos que impactan al negocio, limitándolo a un conjunto de criterios específicos y tangibles, siendo un método selectivo en donde debe tomarse en consideración que existen relaciones causa-efecto entre las diferentes perspectivas. Por ejemplo, la perspectiva financiera medida por valor de la acción, beneficio, ingresos y costo de capital; de clientes medida por market share, satisfacción del cliente y percepción de servicio al cliente; interna medida por el cumplimiento de normativas; de crecimiento medida por ventaja competitiva y reputación.

- Criterios según Westerman 4 'A's: el marco 4A[5], define el riesgo de TI como la posibilidad de acontecimiento imprevisto de un evento que amenaza los objetivos de la empresa relacionados entre sí: agilidad (agility), precisión (accuracy), acceso (access) y disponibilidad (availability).

- Criterios según COSO-ER: COSO-Enterprise Risk Management, se basa en cuatro categorías de objetivos: estrategia, operaciones, información y cumplimiento; enfocándose en que los objetivos del negocio deben estar alineados a la estrategia, la eficiencia y eficacia operativa garantizando el rendimiento y la rentabilidad, la fiabilidad de la información tanto interna como externa, así como la financiera y no financiera, y la adhesión al cumplimiento de leyes, normativas y reglamentos.

[5] Westerman, G.; Hunter, R. *IT Risk: Turning Business Threats Into Competitive Advantage*. USA: Harvard Business School Press, 2007. 240 p.

- Criterios según FAIR: este método se orienta a la seguridad y los criterios de impacto que define, se aplican a todos los riesgos relacionados con TI. Los criterios analizados por FAIR son: productividad, (costo de) respuesta, (costo de) remplazo, ventaja competitiva, aspectos legales y reputación.

1.3. Gestión del riesgo tecnológico

Debido a que un riesgo está sujeto a futuros acontecimientos de los cuales no tenemos conocimiento y su impacto puede verse limitado por las acciones acumulativas que se realicen para poder mitigarlo, es necesario que se realicen actividades planificadas para gestionarlo y así minimizar el impacto llevándolo hasta umbrales de tolerancia aceptados por la empresa, en donde este no exponga a la organización ó, cuyo impacto sea minino de tal forma que no paralice las operaciones de la organización.

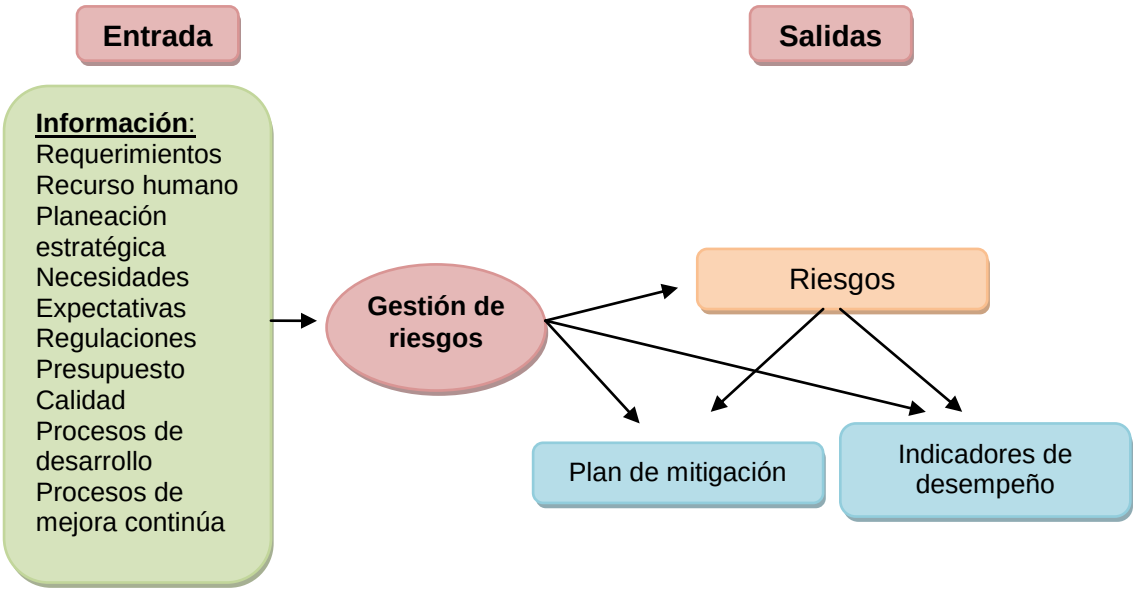
La gestión del riesgo incluye diferentes etapas y este a su vez, consiste en un proceso cíclico que inicia con la recolección de información que se obtiene de diferentes medios y fuentes. De esta información se identifican los riesgos para luego proceder a analizarlos y priorizarlos.

Identificados los riesgos con su periodicidad, nivel de criticidad y tipificados, se procede a realizar un plan de mitigación para luego ejecutarlo y monitorearlo con el objetivo de dar continuidad al ciclo de mejora continua, mitigando de esta forma los riesgo y llevándolos hasta los niveles de tolerancia definidos por la empresa.

El resultado de la etapa de análisis, priorización y evaluación, es un plan de respuesta ante los riesgos priorizados con un conjunto de indicadores que se

utilizaran para medir el éxito del proceso y en su defecto, mejorarlos cuando correspondan como se visualiza en la figura 5.

Figura 5. **Gestión de riesgos: entradas y salidas**



Fuente: elaboración propia.

1.3.1. Identificación de riesgos

Se basa en un levantado de información el cual se puede realizar por medio de entrevistas, encuestas, revisión de información existente, reportes e informes de auditora tanto interna como externa, investigación de regulaciones y normativas a las cuales se encuentre sujeta la empresa y uso de evaluaciones previas.

El objetivo principal de esta actividad es identificar los activos que deben evaluarse para determinar sus amenazas y las vulnerabilidades a las cuales se

encuentran expuestos, logrando identificar las amenazas potenciales que pueden impactar en el negocio ocasionando pérdidas, daño o incumplimiento de objetivos estratégicos.

1.3.2. Análisis o evaluación de riesgos

El análisis de riesgos consiste en un proceso sistemático para medir el impacto y la probabilidad de ocurrencia de cada uno de los escenarios de riesgo identificados. Para el análisis, es indispensable contar con un listado de riesgos identificados que se encuentren clasificados según su grado de afectación y estimación de su recurrencia utilizando para el efecto información relacionada como lecciones aprendidas, estimaciones de costos, planificaciones o correcciones.

Esta actividad es subjetiva y su éxito depende de la experiencia y sensibilidad de la persona responsable del área que se evalúa dentro de la empresa, debiendo tomar en consideración realizar aproximaciones cualitativas o cuantitativas para determinar las probabilidades de ocurrencia, así como el impacto que tendría si el riesgo llegara a materializarse. Al finalizar esta actividad, deberá proporcionarse un mapa de riesgos como el que se muestra en la tabla I, controles para mitigación de los riesgos y niveles de aceptación o tolerancia de la empresa de acuerdo a la exposición al riesgo identificado.

Dentro de los controles a proporcionar en esta etapa, deberán incluirse como mínimo controles preventivos y correctivos, pudiendo llegar a considerar la inclusión de controles defectivos, manuales y automatizados.

Tabla I. **Mapa de riesgos según su impacto y probabilidad de ocurrencia**

		Impacto				
		MINIMO	BAJO	MODERADO	ALTO	CRITICO
Probabilidad de Ocurrencia	ESPERADO	Medio	Medio	Alto	Extremo	Extremo
	MUY PROBABLE	Moderado	Medio	Medio	Alto	Extremo
	PROBABLE	Moderado	Moderado	Medio	Alto	Alto
	POCO PROBABLE	Bajo	Moderado	Medio	Medio	Alto
	REMOTO	Bajo	Bajo	Moderado	Medio	Medio

Fuente: elaboración propia.

1.3.3. Priorización de riesgos

Identificados y tipificados los riesgos, se procede a clasificar los riesgos para determinar cuáles serán gestionados considerando que los recursos son limitados; por lo cual, aquellos que se elijan deberán ser los abordados con los recursos con que cuenta la empresa los cuales deberán ser designados para el efecto, con el objetivo de mitigar la exposición a los mismos y con el enfoque de atacar los riesgos mas grandes o críticos a un costo óptimo.

En esta actividad es importante tomar en consideración la tolerancia al riesgo definida por la empresa y por cada uno de los riesgos, se deberá definir el tratamiento que se dará, pudiendo ser reducción del riesgo, retención del riesgo, evasión del riesgo o transferencia del riesgo. Como resultado, se estaría

proporcionando un listado de oportunidades para el negocio y los riesgos priorizados con el tratamiento que se dará a cada uno.

1.3.4. Mitigación de riesgos

Para mitigar el riesgo, se establece un plan de mitigación el cual deberá proporcionarse a la alta gerencia con la finalidad que se evalúe la exposición al riesgo que presenta la empresa y las propuestas de mitigación o medidas correctivas que pueden implementarse.

El plan de mitigación deberá ser un informe que presente las diferentes alternativas de mitigación, para los casos que aplique, debiendo considerar costos y tiempos de implementación para plantear un panorama más amplio que permita la toma de decisiones.

Este plan de mitigación de riesgos, deberá permitirá la continuidad del negocio considerando los criterios de aceptación previamente definidos como niveles de tolerancia y respuesta por cada uno de los riesgos. Dentro de las recomendaciones a considerar para mitigar estos riesgos, deben considerarse la definición de una política de continuidad del servicio, baselines de continuidad, procedimientos de recuperación y guidelines de continuidad.

1.3.5. Monitoreo y control de riesgos

Por último se establecen indicadores para medir la efectividad de los controles establecidos para mitigar el riesgo tecnológico. De preferencia, estas métricas deberán reflejarse en un cuarto de mandos según la metodología BSC, que permita realizar un seguimiento continuo y detallado de la gestión de

riesgos con el objetivo predecir y dar seguimiento para definir niveles de ocurrencia de un riesgo.

Los indicadores definidos, deberán contar con niveles de tolerancia con la finalidad de permitir detectar variaciones en la efectividad de los controles, debiendo considerar niveles no tolerables, mínimos o tolerables y, aceptables o esperados. De acuerdo al nivel de madurez de la empresa, deberán considerarse métricas de implementación, de efectividad/eficiencia y métricas de impacto.

1.3.6. Cultura del riesgo

La gestión del riesgo consiste en tener un adecuado control y manejar de forma correcta los riesgos a los cuales se encuentra expuesta una organización para ayudarlas a asumir mayores riesgos en búsqueda de la rentabilidad. Una cultura de riesgos se logra cuando los diferentes niveles de la organización conocen y se encuentran conscientes de cómo y porque deben responder antes los eventos adversos de TI que puedan ocurrir; partiendo de la parte superior de la estructura organizacional, desde la junta directiva y ejecutivos del negocio, con una comunicación clara a los niveles inferiores para fomentar el aprendizaje y entendimiento a los diferentes niveles así como su accionar en pro del tratamiento de los riesgos como parte de sus operaciones.

Para una adecuada gestión de la cultura de riesgos debe considerarse:

- Comportamiento hacia la toma de riesgos: debe entenderse, ¿cuál es el grado de riesgo que puede absorber la organización, y cuál es el riesgo que está dispuesta a asumir?

- Comportamiento hacia la política: ¿en qué medida el personal aceptara el cumplimiento de la política?

- Comportamiento hacia resultados negativos obtenidos: ¿cómo reaccionara la empresa ante los resultados negativos, como eventos de pérdida o perdida de oportunidades?, ¿qué enfoque tomara?, se aprenderá de los errores y se adaptara el modelo o se buscara un culpable sin tratar de corregir la causa raíz.

La figura 6, muestra los elementos de la cultura de riesgos.

Figura 6. **Elementos de la cultura de riesgos**

Fuente: Framework Risk IT Based on COBIT®.

Los principales síntomas de una cultura de riesgos inadecuada comprenden una desalineación entre el apetito de riesgos definido y la traducción de estas en las políticas implementadas, así como la existencia de una cultura de culpas en lugar de corregir el problema. Por ejemplo, puede ser que la organización toma la decisión de asumir los riesgos mientras que esto no se refleja de la misma forma en la política donde pudiera reflejarse que la organización es más exigente.

Asimismo, es necesario que en la organización se fomente la cooperación de tal forma que los indicios de búsqueda de culpables se elimine ya que esto es un inhibidor para lograr la comunicación clara, relevante y eficaz, en una cultura de culpa normalmente las unidades del negocio tienden a señalara a las áreas de tecnología como causa del fracaso, esto se nota más en proyectos de TI cuando no son entregados en tiempo o no cumplen con las expectativas; por lo cual es de relevancia hacer ver a las unidades del negocio que son parte fundamental de los proyectos desde sus inicios para alcanzar el éxito.

1.4. Marco de referencia Risk IT

Risk IT es un marco basado en guías, principios, procesos de negocio y directrices de gestión implementadas para la gestión eficaz de los riesgos de TI; establece las mejores prácticas con el fin de proporcionar a las empresas un marco de referencia para identificar, gobernar y administrar los riesgos asociados a su negocio, logrando con esto una mejor gestión de riesgos de TI; para el efecto, se basa en los principios de gestión de los riesgos organizacionales (ERM), normas y marcos como COSO ERM[6] y AS/NZS 4360[7],

[6] Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework*.

[7] Standards Australia, AS/NZS 4360:2004. *Australian/New Zealand Standard for Risk Management*.

los cuales encuentran en proceso de sustitución por la norma ISO 31000, el dominio británico ARMS5, entre otros.

El marco Risk IT promueve la gestión del riesgo tecnológico como parte de la cultura de la organización para poder asumir mayores riesgos en busca de la rentabilidad; para lograrlo, se basa en la gestión del riesgo y la comunicación para que esta gestión se dé acorde a las necesidades del negocio con el fin de mitigar la exposición a los riesgos que presenta la misma, dentro de los niveles de tolerancia definidos por la dirección ejecutiva y del consejo.

También brinda una guía para que el flujo de comunicación sea el adecuado exponiendo los componentes de entrada y salida que deben generarse para la gestión del riesgo tecnológico de tal forma que estos se expresen en términos claros e inequívocos para él negocio.

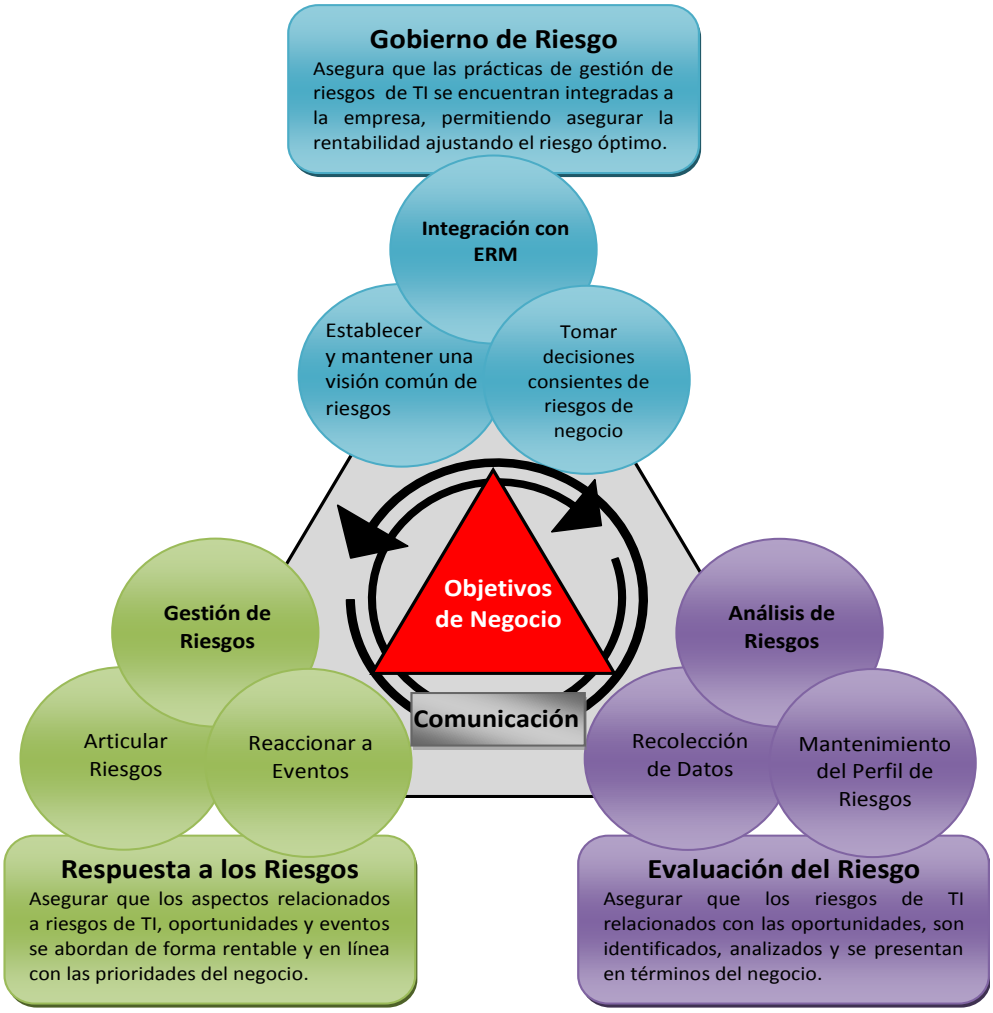
El marco Risk IT basado en que la gestión de riesgos es una práctica global y debiera ser considerado como uno de los requisitos estratégicos en las organizaciones, se encuentra destinado a un público amplio incluyendo ejecutivos o miembros del consejo, encargados de TI y departamentos de negocio que se encuentran involucrados en sus procesos a la gestión y uso de tecnología, profesionales dedicados a la gestión de riesgos que necesitan una guía para gestionar riesgos de TI y publico externo interesado.

Según la definición del marco Risk IT, el riesgo se compone de los eventos relacionados con TI que potencialmente pueden llegar a afectar al negocio. Este hecho tiene una probabilidad de ocurrencia con una frecuencia e impacto incierto para la organización y supone que generara dificultades a la organización para alcanzar sus resultados definidos en base a metas y objetivos estratégicos.

1.4.1. Estructura Risk IT

El marco RISK IT se conforma por tres dominios para los cuales se enfocan en el gobierno de riesgos, la evaluación del riesgo y la respuesta al riesgo; cada uno se compone de tres procesos como se muestra en la figura 7; a su vez, cada proceso por actividades para la gestión de riesgos tecnológicos.

Figura 7. **Marco de riesgos de TI**



Fuente: Framework Risk IT Based on COBIT®.

1.4.1.1. Gobierno de riesgos (GR)

El objetivo de este dominio consiste en garantizar que las prácticas de gestión de riesgos tecnológicos se encuentran arraigadas en la empresa, lo que le permite garantizar una óptima rentabilidad de la empresa ajustada al riesgo.

Dentro de las métricas que se implementan para medir el nivel de cumplimiento de este dominio se encuentran:

- Reducción del riesgo global de la empresa por el uso estratégico de TI para generar apalancamiento de los recursos de empresa.

- Porcentaje de personal capacitado en técnicas de gestión de riesgos críticos. Por ejemplo: en estándar de técnicas de análisis de riesgos, gestión de crisis, gestión de proyectos, habilidades de las personas (de auditoría, control, entre otras) para detectar cuando algo anda mal con aspectos relacionados a las TI.

Los procesos que conforman el dominio de la gestión de riesgos son:

- RG1 - establecer y mantener una visión del riesgo común: este proceso busca Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la empresa de TI relacionados con la pérdida de liderazgo y la tolerancia subjetiva de la misma.

- RG2 - integrar con ERM: busca integrar la estrategia y las operaciones de gestión de riesgos de TI con las decisiones estratégicas de riesgo de negocio que se han tomado a nivel de empresa.

- RG3 - toma de decisiones conscientes de los riesgos del negocio: busca asegurar que las decisiones de la organización toman en cuenta la amplia gama de oportunidades y consecuencias generadas de la dependencia en TI para alcanzar el éxito.

1.4.1.2. Evaluación de riesgos (ER)

El objetivo consiste en asegurar que los riesgos relacionados con TI y las oportunidades, son identificadas, analizadas y se presentan en términos del negocio. Para medir el cumplimiento de este dominio se realiza en base al impacto en el negocio acumulado de incidentes y eventos relacionados con las TI que no fueron identificados por los procesos de evaluación de riesgos.

Los procesos que comprenden este dominio son:

- RE1 - recopilar datos: consiste en identificar los datos pertinentes para hacer viable la identificación de riesgos de TI relacionados, el análisis y presentación de informes.

- RE2 - analizar los riesgos: consiste en generar información útil para apoyar las decisiones de riesgo que tomen en cuenta factores de riesgo de negocio.

- RE3 - mantener perfil de riesgos: consiste en actividades para mantener actualizado un inventario completo de riesgos y atributos conocidos (como frecuencia esperada, impacto potencial y disposición), los recursos de TI, capacidades y controles según se entiende en el contexto de productos, servicios y procesos del negocio.

1.4.1.3. Respuesta de riesgos (RR)

El objetivo de este dominio es garantizar que los temas de riesgo relacionados con TI, las oportunidades y los eventos se abordan de una manera rentable considerando el costo/eficacia y de acuerdo con las prioridades del negocio.

El cumplimiento de este dominio se mide en base al impacto acumulado en el negocio de incidentes y eventos relacionados con TI previstos por los procesos de evaluación del riesgo, pero aún no abordados por el plan de mitigación o acciones a realizar sobre eventos.

Los procesos que comprenden este dominio son:

- RR1 - articular el riesgo: por medio de este proceso se busca garantizar que la información sobre el estado real de las exposiciones y las oportunidades relacionadas con la TI se pone a disposición en forma oportuna y a las personas adecuadas para una respuesta adecuada.

- RR2 - gestionar el riesgo: su objetivo es garantizar que las medidas para aprovechar las oportunidades estratégicas y reducir los riesgos a un nivel aceptable se gestionan como un portafolio.

- RR3 - reaccionar a acontecimientos: su objetivo es asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con TI se activan de forma oportuna y eficaz.

Para lograr implementar la gestión de riesgos de TI en una empresa basada en Risk IT debe evaluarse las actividades que aplican para cada empresa y, cada una de las actividades definidas como aplicables de los procesos que conforman los tres dominios del marco de referencias Risk IT, deberá ser ejecutada por diferentes roles de la empresa buscando que estos se gestionen a todo nivel dentro de la organización. Para tener una guía de referencia que permita identificar las responsabilidades de cada rol y sus funciones, se recomienda revisar los cuadros RACI[8] definidos en el Framework Risk IT para cada una de las directrices adoptadas.

1.4.2. Público y partes interesadas al que se dirige Risk IT

Como se ha mencionado, el marco de Risk IT ha sido enfocado a un amplio púbico por los beneficios y valor agregado que ofrece a cada uno de ellos. Las partes interesadas para la gestión de riesgos de TI que se ven beneficiadas por el marco Risk IT, se listan a continuación:

- Junta y dirección ejecutiva: brinda una mejor comprensión de sus responsabilidades y funciones a desempeñar con respecto a la gestión de riesgos de TI.

- Gestores de riesgos: brinda asistencia con la gestión de riesgos de TI, generalmente, de acuerdo a la organización que representan y de acuerdo a los principios de la gestión de riesgos.

[8] RACI por sus siglas en inglés, identifica quién es responsable (Responsible), rinde cuentas (Accountable), consultado (Consulted) y / o informado (Informed).

- Administradores de riesgos operacionales: brinda un marco de referencia que vincula los riesgos de TI, identificando pérdidas operativas y principales indicadores de riesgo.

- Dirección de TI: permite comprender como identificar y gestionar los riesgos asociados a TI y como comunicarlos para la toma de decisiones del negocio.

- Directores de servicios de TI: mejora el punto de vista sobre los riesgos relacionados con TI, debiendo encajar en el conjunto global del marco de trabajo de la gestión de riesgos de TI.

- Administradores de continuidad de negocio: permite alinear con la organización la gestión de riesgos, siendo la evaluación del riesgo un aspecto clave de su gestión.

- Administradores de seguridad de TI: permite posicionar los riesgos de seguridad entre otras categorías de riesgos de TI para poder priorizarlos y atacarlos.

- CFOs: permite obtener una mejor visión de los riesgos relacionados con TI y el impacto financiero que estos representan para el negocio.

- Oficiales de gobierno organizacional: brinda asistencia para las evaluaciones de supervisión que realizan como parte de la responsabilidad de gobierno de TI.

- Directores ejecutivos: permite dar claridad en el impacto y relación que tienen los riesgos de TI y como estos forman parte de los riesgos de negocio.

- Auditores de TI: permite mejorar el análisis de riesgos en apoyo a los planes de auditoría e informes que generan en las mismas relacionados a evaluaciones de riesgos.

- Reguladores: permite dar un enfoque de gestión de riesgos de TI a las evaluaciones que realizan a organizaciones reguladas. En nuestro medio podemos mencionar las evaluaciones que realiza la Superintendencia de Bancos al sector financiero.

- Auditores externos: brinda una guía adicional para evaluar los niveles de riesgo relacionados con TI al momento de establecer un dictamen sobre la calidad de control interno.

- Aseguradores: apoyo en el establecimiento de coberturas de seguro adecuados de TI y la búsqueda de un acuerdo sobre los niveles de riesgo.

- Agencias de calificación: brinda una referencia para evaluar y puntuar objetivamente como una empresa se ocupa de los riesgos de TI, esto en colaboración con las aseguradoras.

1.4.3. Principios del riesgo de TI

El marco Risk IT ha sido diseñado para cumplir con principios que le permiten tener un control adecuado de los riesgos a lo largo de los modelos organizacionales dentro de los cuales tenemos:

- Alinear con los objetivos organizacionales: uno de los factores claves para el éxito de la gestión del riesgo de TI es que estos estén alineados a los objetivos del negocio, de tal forma que estos sumen al cumplimiento de los objetivos del negocio protegiendo contra la destrucción de valor y generando valor.

- Alinear la gestión de riesgos organizacionales relacionados con las TI con ERM: permitiendo tener una claridad en relación a los objetivos del negocio, riesgos y niveles de tolerancia, así como el apetito al riesgo e integración de los departamentos de la organización por medio de la comunicación y expansión de la gestión a todos los niveles.

- Balance de costos y beneficios de la gestión de riesgos de TI: permitiendo priorizar y dirigir los riesgos en relación al apetito del riesgo y sus niveles de tolerancia, establecer controles buscando eficiencia y un mejor rendimiento costo-beneficio.

- Promover la comunicación equitativa y abierta de los riesgos de TI: la comunicación es muy importante de tal forma que se expanda la gestión de riesgos a través de toda la estructura de la organización. Permitiendo integración, una clara difusión y conclusiones técnicas en términos del negocio.

- Establecer el tono correcto desde arriba hacia abajo, definir responsabilidades del personal y hacer cumplir los niveles de tolerancia aceptables para el negocio, especialmente creando cultura de riesgo, iniciando desde los niveles más altos e identificando personas claves para que gestionen el riesgo de IT, toma de decisiones y, divulgación de acciones por medio de políticas, procedimientos y definición de niveles de ejecución.

- Fomentar el proceso de mejora continua y hacerlo parte de las actividades diarias, con el objetivo de contar con un proceso iterativo para gestionar el riesgo considerando que estos son dinámicos, debe contarse con prácticas simples y fáciles de utilizar que permitan detectar amenazas y riesgos potenciales con el fin de prevenirlos y mitigarlos; para el efecto se deben establecer métodos, funciones y responsabilidades, herramientas, técnicas y criterios para manejarlos en toda la organización, así como la integración en orden de prioridad con los procesos de toma de decisiones de la organización.

1.4.4. Fundamentos de la evaluación del riesgo de TI

Para una adecuada evaluación de riesgos, es necesario que se describa el impacto que tiene el riesgo sobre la organización y los diferentes escenarios de riesgos a los cuales se encuentra expuesta la misma. La descripción del riesgo y su impacto no es más que expresar de forma clara en términos relevantes para el negocio la exposición al riesgo y del por qué estos deben ser gestionados a tal grado que todas las partes interesadas tengan la capacidad de comprender, asimilar y expresar como los acontecimientos adversos pueden impactar los objetivos del negocio.

Al describir el riesgo, se debe garantizar:

- Que una persona del negocio entienda como los fallos en TI afectan los servicios y procesos claves, principalmente, como estos pueden impactar en los objetivos del negocio.

- Que el personal de TI comprenda como los fallos de TI pueden impactar en el cumplimiento de los objetivos del negocio, causando pérdidas directas o indirectas.

Para una adecuada comprensión de los eventos adversos, expresando el vínculo de TI con el impacto de escenarios de riesgo organizacional en un lenguaje en términos del negocio, existen diferentes técnicas las cuales fueron citadas en el apartado 1.2.4 correspondiente al Impacto que presenta el riesgo tecnológico para una organización.

La identificación de escenarios es otro factor importante para la evaluación de riesgos, cuya actividad es un desafío para la gestión de TI ya que deben identificarse los riesgos importantes y relevantes para el negocio determinándolos de todo aquello que puede relacionarse con TI y considerando la presencia, así como la dependencia de TI en el negocio. Durante la identificación de riesgos, se definen eventos relacionados con TI que pueden impactar en el negocio cumpliendo con los componentes descritos en el apartado 1.2.3.

Para identificar los riesgos, es muy importante realizar una combinación de mecanismos que se basan en un enfoque de arriba abajo, en donde analizando desde los objetivos generales del negocio se definen escenarios que impacten los objetivos del negocio y, un enfoque de abajo arriba, en donde se

analizan escenarios genéricos que sirven de base para definir escenarios específicos aplicables a la situación de la organización.

Luego de tener identificados los escenarios relevantes, se deben identificar los factores de riesgos; de estos dependerá la frecuencia y/o impacto que pueden tener en la organización al momento de que llegue a materializarse un riesgo.

Dentro de los factores de riesgo se deben incluir los factores externos, factores internos, capacidad de la gestión del riesgo o madurez en la gestión de riesgos basada en Risk IT, capacidades de TI para cumplir con los procesos basada en COBIT y, gestión del valor o alineamiento de TI con el negocio, basadas en Val IT.

1.4.5. Fundamentos de la respuesta de riesgo

Una respuesta al riesgo no es más que llevar el riesgo residual dentro de los límites de tolerancia del riesgo o al mismo nivel del apetito de riesgo definido por la empresa. Para poder dar respuesta a un riesgo al cual se encuentra expuesta una organización es necesario poder medirlos y controlarlos, esto es trabajado por medio de indicadores los cuales permiten saber si una empresa se encuentra sujeta a, o tiene la probabilidad de, estar sometida a un riesgo que se encuentra por arriba del apetito de riesgo definido.

Los indicadores deben definirse de acuerdo a las características de cada empresa, para una correcta definición de indicadores de riesgo, la empresa deberá cumplir con los siguientes pasos que se describen a continuación:

- Identificar Stakeholders o partes interesadas: al considerarlos, no solo deberá enfocarse en las operaciones o estrategia del riesgo, también tomar en consideración como afecta a los diferentes interesados para garantizar una mayor aportación para definir los indicadores.

- Realizar una selección equilibrada de riesgos, considerando indicadores de desempeño (que ha sucedido después de ocurridos los eventos), indicadores principales (capacidad para prevenir los eventos que produzcan) y tendencia (análisis de los indicadores a través del tiempo para establecer comportamientos y tendencias).

- Asegurarse de que los indicadores definidos bajen a nivel de detalle mostrando el origen de los acontecimientos (que permitan identificar el origen y no solo los síntomas).

Debido a que los indicadores claves de riesgo KRIS, son de gran relevancia para le empresa por proveer una alta probabilidad de predecir o por indicar un riesgo importante, deben ser seleccionados de forma cuidadosa considerando:

- Impacto: seleccionar los que tengan mayor impacto comercial.

- Nivel de esfuerzo para aplicar, medir y comunicar: Para riesgos equivalentes, seleccionar el más fácil de medir.

- Fiabilidad: el indicador debe tener una correlación alta con el riesgo y permitir predecir el riesgo o medir su resultado.

- Sensibilidad: el indicador deberá ser representativo del riesgo e indicar las variaciones en el riesgo.

Las respuestas a riesgos dependerán de los recursos y niveles de tolerancia que la empresa esté dispuesta a asumir, por lo cual es importante que se defina por cada riesgo identificado el tratamiento que tendrá en respuesta a su materialización, tomando en consideración las siguientes posibles repuestas:

- Evitar el riesgo: esta respuesta se debe dar cuando el riesgo es juzgado como inaceptable, no puede ser transferido ni compartido y al momento de intentar reducirlo no se ha tenido éxito obteniendo resultados por debajo de los umbrales de tolerancia definidos. Esta respuesta busca salir de las condiciones, situaciones o actividades que dan lugar al riesgo.

- Mitigar o reducir el riesgo: mitigar o reducir un riesgo se enfoca a las actividades que realiza la organización para disminuir la frecuencia o impacto del riesgo en el negocio buscando llevarlos a los niveles de tolerancia aceptables. Esto se logra al implementar medidas de control que permitan identificar los factores y eventos que ocasionan el riesgo buscando disminuirlos y/o corregirlos.

- Transferencia o compartir el riesgo: es una forma de afrontar el riesgo compartiendo la responsabilidad, impacto o inversión en proyectos de riesgos, asumiendo entre la empresa y un tercero la consecuencia del riesgo que pueden ser económicas si se llegara a materializar el riesgo. Esta técnica no mitiga el riesgo sin embargo disminuye el impacto en la organización y muchas veces puede ser adquiriendo un seguro para

mitigar el riesgo para incidentes relacionados a las TI, subcontratar proveedores de proyectos o para realizar actividades de TI que de acuerdo a las negociaciones debieran asumir el riesgo ya sea por penalizaciones o acuerdos de servicio.

- Aceptar el riesgo: aceptarlo significa asumir las consecuencias que conlleva la materialización del riesgo; a diferencia de ignorarlo en este caso se conoce el riesgo, sus consecuencias e impacto, y de acuerdo al análisis de riesgos se establece que la empresa puede aceptarlo, lo cual debe ser definido por la dirección de los procesos de negocio relacionados en apoyo con TI. El adoptar esta postura requiere que se defina el responsable o área responsable que asumirá el riesgo debiendo comunicar tal decisión ante la junta responsable de la empresa.

Para poder definir el tipo de respuesta que será dado a un riesgo de TI, es necesario que la empresa tome en consideración diferentes criterios para lo cual se recomienda responder las siguientes interrogantes:

- ¿Cuál es el costo para dar respuesta al riesgo? dependiendo del tipo de respuesta la organización deberá realizar actividades que tienen un costo y requerirán inversión de recursos; por ejemplo el costo del pago de una prima de seguro, contratar personal para implementar un plan de mitigación, entre otros.

- ¿Qué impacto representa el riesgo ante el negocio? esto se determina de la matriz de riesgo en donde se puede observar la frecuencia y la magnitud de cada riesgo.

- ¿Qué madurez tiene la empresa para mitigar el riesgo? dependiendo del nivel de madurez de la empresa, dependerá la capacidad de respuesta al riesgo con lo cual mientras más alto sea el nivel de madurez se podrán implementar medidas más sofisticadas, caso contrario sucede al estar en un nivel bajo en cuyo situación una respuesta básica puede ser de mayor beneficio para la empresa.

- ¿Qué beneficios se esperan obtener? analizado tanto a nivel de eficiencia que corresponde a los beneficios que obtendría la empresa y, eficacia que se centra en determinar si se reducirá el impacto o frecuencia del riesgo; si los beneficios son mínimos no es recomendable invertir demasiados recursos.

1.4.6. Beneficios de implementar Risk IT

El marco de referencia Risk IT aporta muchas ventajas a una empresa permitiéndoles cubrir una diversidad de factores que generan beneficio para los resultados de las organizaciones, impactando en sus operaciones, resultados y diferentes factores, proveyendo:

- Una visión de la situación actual y del futuro sobre los riesgos de TI de la organización, asimismo refleja el éxito de la organización en relación a la gestión de sus riesgos.

- Proporciona una guía para gestionar los riesgos de TI de principio a fin cubriendo más allá de aspectos técnicos de control y de seguridad.

- Comprensión de cómo capitalizar una inversión de un sistema de control interno de TI ya existente para gestionar los riesgos relacionados a las TI.

- Integración de la evaluación y gestión de riesgos de TI, con el riesgo global de la empresa cumpliendo las estructuras de la organización.

- Lenguaje común para comunicarse a nivel de los ejecutivos responsables de la toma de decisiones, el director de información y la organización de gestión de riesgos, o entre los auditores y la dirección.

- Promueve la definición y asignación de responsabilidades de riesgo y su aceptación en todos los niveles y áreas de la organización.

- Provee un perfil de riesgos completo para entender de una mejor forma los riesgos y aprovechar los recursos de la organización.

2. NIVEL DE MADUREZ DE UNA PYME EN LA GESTIÓN DEL RIESGO TECNOLÓGICO

La implementación de Risk IT en una empresa por ser un marco de referencia, permite que sea personalizado de acuerdo a las necesidades para lo cual deben analizarse los componentes del marco y adoptar los que se acoplen a la organización.

Como primer paso, debe evaluarse el nivel de madurez que tiene la empresa para mitigar el riesgo tecnológico debiendo identificar inicialmente la situación actual de la misma.

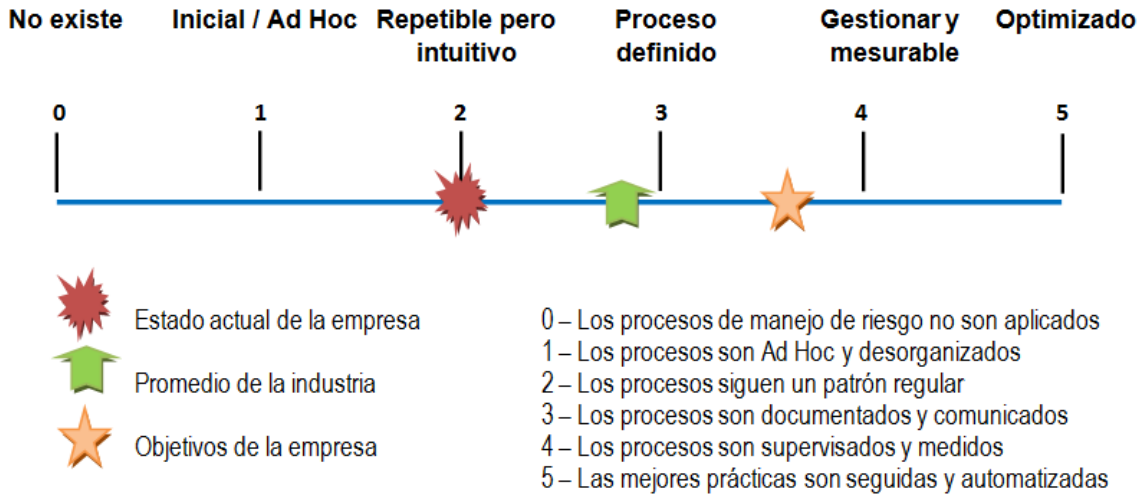
En nivel de madurez de gestión de riesgos permite determinar que tan preparada se encuentra la empresa para gestionar los riesgos tecnológicos a los cuales se encuentra expuesta; el nivel de madurez dependerá, del nivel de dependencia que tiene la empresa de las TI, su nivel de sofisticación tecnológica y el futuro del papel ejecutivo que se tiene para prever la gestión de la tecnología de la información. El nivel adecuado de madurez para una empresa, se ve influido por la misma empresa, los objetivos del negocio, el entorno operativo y las prácticas de la industria.

2.1. Nivel de madurez

Basados en COBIT 5, el nivel de madurez se mide en base a las capacidades de los procesos de acuerdo a seis niveles claves lo cual ayuda a la organización a identificar si existen deficiencias y a partir de ellas establecer objetivos para mejorar la gestión cuando sea necesario.

La figura 8, muestra los niveles de madurez definidos por COBT 5 para la medición del nivel de madurez de un proceso, en nuestro caso implementado para la gestión del riesgo tecnológico.

Figura 8. **Modelo de madurez**



Fuente: Framework Risk IT Based on COBIT®.

- Nivel 0 – no existe: en este nivel la empresa no ha implementado ningún proceso para gestionar el riesgo o no ha logrado alcanzar su propósito. No se cuenta con evidencias de logros obtenidos y posiblemente la organización no ha reconocido los riesgos por lo cual no existe comunicación alguna de los mismos y no se tiene consciencia de la necesidad de implementar controles ni se cuenta con la capacidad para reaccionar ante el riesgo buscando limitar la frecuencia y el impacto de incidentes relacionados con las TI.

Este es un escenario de caos para las empresas ya que no cuentan con procedimientos para atender los riesgos y estos tampoco han sido identificados.

- Nivel 1 – proceso iniciado o Ad Hoc: en este nivel la mayoría de procesos son Ad Hoc y caóticos, la empresa realiza acciones para mitigar el riesgo reconociendo las necesidades de reaccionar ante estos, sin embargo se limitan solamente a evitarlos cumpliendo con requisitos o transfiriendo el riesgo ya sea a través de la adquisición de seguros o compartiendo el riesgo con algún proveedor.

  Usualmente no se provee un ambiente estable para soportar los procesos y existe una consciencia mínima de la amenaza y acciones a realizar si el riesgo se materializa; asimismo, las responsabilidades son mínimas para gestionar el riesgo no garantizando que las medidas sean las adecuadas. El éxito se debe a la competencia y esfuerzo de personal en la organización y no al uso de procesos probados o definidos; se ejecutan procesos desorganizados, exponiendo a la empresa al riesgo que pueden afectar la operación si al ser atendidos, no se da una respuesta a la operación que considere la eliminación del riesgo.

  A pesar del caos, la empresa lanza productos que funcionan, sin embargo estos exceden su presupuesto y no cumplen sus planes; otro factor que las caracteriza es que no se comparten conocimientos ni métodos de trabajo por lo cual, si una persona clave se retira se pierde el conocimiento para la empresa.

  En el nivel 1, se cuenta con controles implementados, enfocados al cumplimiento de requisitos del negocio que han sido aplicados de forma

aislada lo cual puede ocasionar que áreas diferentes controlen sus riesgos de forma independiente.

Este nivel, denota una falta de habilidades y competencias por parte de la organización para reaccionar ante el riesgo lo cual expone a la empresa a aceptar riesgos que se encuentran fuera de los umbrales de tolerancia definidos.

- Nivel 2 – proceso manejable: en este nivel se pone en orden el caos, se tiene consciencia individual de las amenazas con definición de puntos de contacto para reaccionar ante el riesgo si estos se materializan; existe una comunicación de los riesgos y las respuesta ante estos se ve afectada por un lenguaje de negocio de una unidad específica y por competencia entre áreas.

  En el nivel 2, la organización cuenta con procesos definidos para la ejecución de proyectos, los cuales se encuentran planificados y ejecutados de acuerdo a políticas y lineamientos establecidos; se involucra a las partes interesadas, se monitorea, controla, revisa y evalúa de acuerdo a las directrices definidas en los procedimientos. En este nivel se presenta un líder emergente para la respuesta al riesgo quien asume la responsabilidad para mitigarlos y apoya la gestión del impacto.

  Regularmente los riesgos presentan un patrón, los cuales normalmente ocurren cuando se trabaja sobre la implementación de controles para mitigarlo; se cuenta con requisitos mínimos para formar áreas críticas que gestionan el riesgo y es posible que se detecten deficiencias en los controles que no son atendidos de forma oportuna ya que este nivel solamente intuye los riesgos.

Las áreas tienen un enfoque común para el uso de herramientas de mitigación y respuestas de riesgos que han sido definidos por personal clave del negocio pero que no se encuentran integrados entre ellos.

- Nivel 3 – proceso definido: al igual que el anterior, se tiene una consciencia de las amenazas con la diferencia que acá se comprende el impacto que representa para el negocio y las acciones concretas que deben realizarse si el riesgo llegara a materializarse. Un beneficio fundamental que se tiene en el nivel 3, es que los procesos se encuentran debidamente documentados y son comunicados a los diferentes niveles de la organización, asimismo, los procesos se encuentran estandarizados de tal forma que aplican para todo proyecto, a diferencia del nivel 2 en donde pueden existir procesos por proyecto los cuales difieren entre ellos.

  El nivel 3 requiere que los procesos se definan claramente planteando el propósito, entradas, criterios de entrada, actividades, roles, medidas, pasos de verificación, salidas y criterios de salida, asimismo que sean manejados proactivamente entendiendo las interrelaciones de las actividades y medidas detalladas del proceso, sus artefactos y sus servicios

  En este nivel se identifican los dueños de los procesos claves y se establecen responsabilidades para la comunicación de las respuestas al riesgo. Difiere del nivel 2 en que al identificar las deficiencias en controles, estas son corregidas de forma oportuna; se incluye dentro de la política de la empresa los procedimientos para respuesta al riesgo y esto se llega a definir a nivel de puestos de trabajo para que se tengan claras las expectativas de respuesta al riesgo.

Bajo este modelo de respuesta al riesgo, se observa capacitación constante del personal para gestionar las amenazas y riesgos relacionados a TI, escenarios de riesgo y controles relacionados a sus funciones y responsabilidades. Se cuenta con herramientas para automatizar la reducción de riesgos y se cuenta con un plan para realizarlo.

- Nivel 4 – proceso gestionado o manejado cuantitativamente: la empresa cuenta con un proceso de gestión de riesgos planificado, supervisado y ajustado, donde sus resultados se encuentran definidos, controlados y son mantenidos; se tiene una comprensión individual y organizativa de requisitos para gestionar los riesgos. Hay involucramiento de la alta gerencia que con apoyo de la gestión de TI determinan si una condición de riesgos se encuentra o no en los umbrales de tolerancia.

  Se cuenta con un proceso de medición de la eficiencia y eficacia de respuesta al riesgo que a su vez se encuentran relacionados a los objetivos estratégicos del negocio y estos son comunicados a las áreas de negocio, se encuentran documentados los procesos para responder al riesgo y estos son medidos de forma cuantitativa. Los objetivos cuantitativos se definen en base a necesidades del cliente, usuarios finales, organización y actores de los procesos.

  En este nivel existe un crecimiento, mejora y redefinición que permite actualizar continuamente la gestión del riesgo que incluye la forma de articular el riesgo, mitigación, reacción ante la materialización del mismo y aprovechamiento de las oportunidades que conlleva la mitigación; para esto se utilizan los controles para establecer causas comunes de variación en los procesos y así modificar los procesos para

alcanzar mejores resultados. Se utilizan herramientas para gestionar el riesgo de cartera del negocio, supervisar los controles, recursos y capacidades de la empresa.

- Nivel 5 – proceso optimizado: el proceso definido para la gestión del riesgo es mejorado continuamente a través de mejoras continuas, incrementales y tecnológicas, de tal forma que cumple con las metas y requisitos del negocio presentes y futuros. Se implementan mejores prácticas para la gestión del riesgo y se automatizan controles.

  Se cuenta con una estrategia para dar respuesta al riesgo, aplicando de forma integral las estrategias y se aplican controles que consideran el costo-beneficio para mitigar el riesgo continuamente, analizando que la inversión sea justificable para la empresa. A diferencia del nivel 4 que se orienta a encontrar causas de variación y proveer una predicción estadística de los resultados, el nivel 5 se enfoca en causas comunes de variación de procesos para mejorarlos.

  En el nivel 5, la empresa fomenta la mejora continua de las capacidades de la empresa para responder a los riesgos sobre la base de tener una clara definición de objetivos individuales y organizacionales; se implementan tecnologías que permiten asumir riesgos adicionales y aprovechar nuevas oportunidades para analizar los impactos y, beneficios de tolerar los riesgos y mantenerlos bajo los umbrales definidos.

2.2. Metodología para determinar el nivel de madurez

Definidos los niveles sobre los cuales determinaremos la situación actual para gestionar el riesgo, procedemos a definir la metodología bajo la cual realizaremos el análisis del nivel de madurez de la empresa.

Dado que la propuesta corresponde a emplear el marco de referencia Risk IT y con el objetivo de detectar oportunidades de mejora, se procede a realizar una evaluación de una PYME basado en los dominios que cubre el marco Risk IT la cual se realizara por medio de una serie de preguntas puntuales que permiten establecer la frecuencia con la cual se realizan ciertas actividades relacionadas a la gestión de riesgos.

La evaluación se centrara solamente en determinar el nivel de madurez de la empresa para gestionar el riesgo no incluyendo en la evaluación el determinar si la empresa cuenta con un modelo de mejora para la definición de procesos de desarrollo y mantenimiento de software como CMMI o mejores prácticas de la gestión de operaciones de TI como ITIL. Tampoco será incluida la identificación de riesgos puntuales ni el nivel de exposición a cada uno de estos riesgos, sin embargo, se proveerá un plan de acción para minimizar la exposición al riesgo tecnológico definiendo actividades puntuales a realizar por la empresa para gestionar el riesgo.

La recopilación de datos será por medio de entrevistas a los principales roles de la organización relacionados a la gestión de TI y la gestión de riesgos de TI, con la finalidad de tener un mejor enfoque o panorama de la situación actual de la PYME en relación a la gestión de riesgos relacionados a TI.

Para determinar la frecuencia con que se realizan las actividades relacionadas a la gestión de riesgo, trabajaremos utilizando una escala de 5 posibles niveles los cuales se citan en la tabla II.

Tabla II. **Niveles para medir la frecuencia de ejecución de actividades de la gestión de riesgos**

Nivel	Valor
Nunca	0
Rara vez	1
A veces	2
Frecuentemente	3
Siempre	4

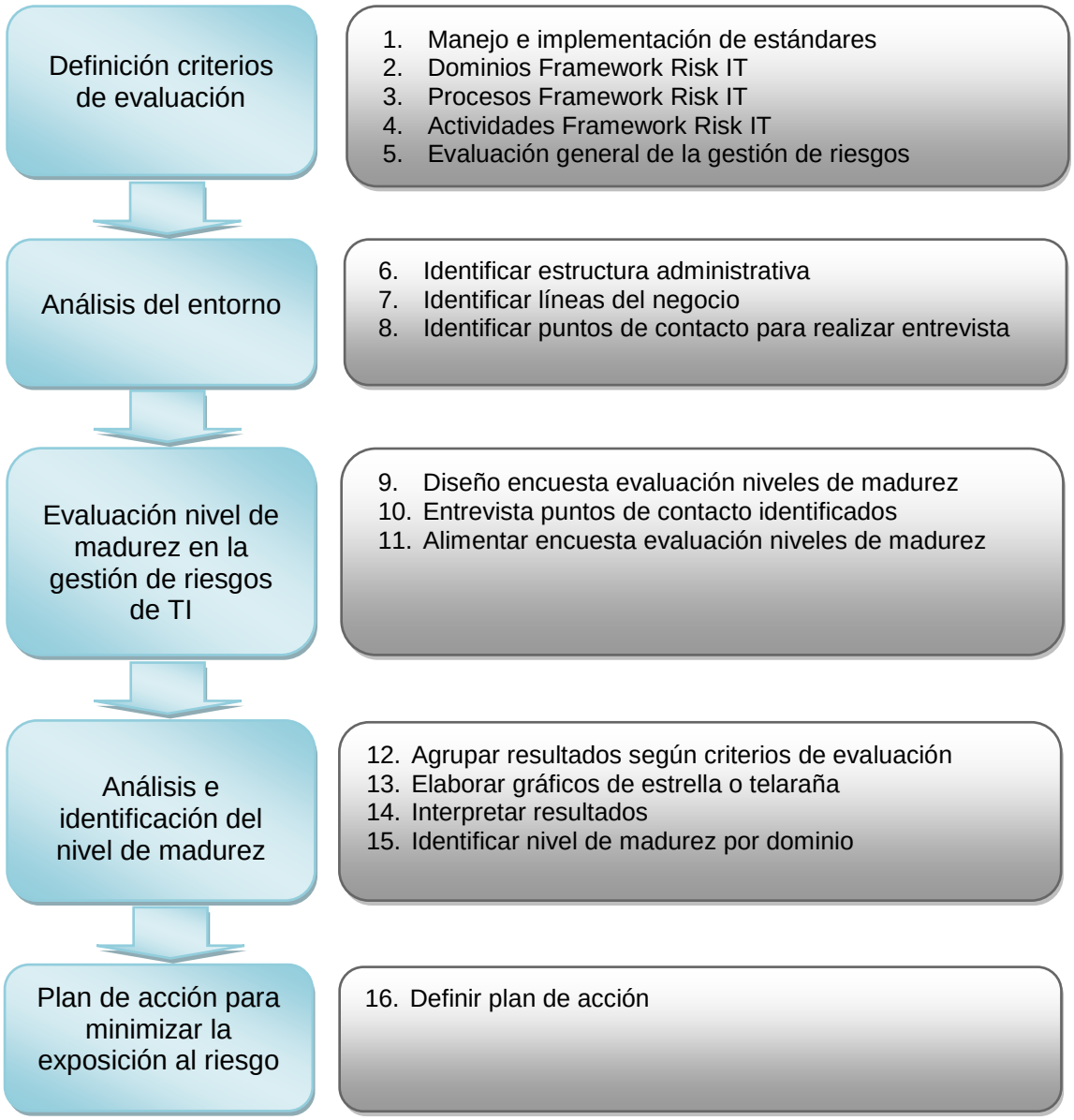
Fuente: elaboración propia.

Para realizar el análisis, se procederá a determinar el entorno realizando un análisis de la empresa enfocado en los tres dominios definidos en el marco de referencia Risk IT para la gestión de riesgos, esto nos permitirá determinar el nivel de madurez por cada uno de los dominios, siendo estos el gobierno de riesgos, evaluación de riesgos y respuesta al riesgo; asimismo, se procederá a evaluar las líneas del negocio de la PYME para determinar los roles e interesados en la gestión de riesgos de TI.

Los resultados de la encuesta serán representados en diagramas radiales o de telaraña lo cual permitirá medir la frecuencia de ejecución de actividades de acuerdo a los criterios evaluados y según la frecuencia de ejecución definidos en la tabla II.

La figura 9, muestra el flujo de trabajo a ejecutar para determinar el nivel de madurez y establecer el plan de acción para minimizar la exposición a riesgos.

Figura 9. **Proceso evaluación modelo de madurez**



Fuente: elaboración propia.

Al determinar el nivel de madurez, se establecerá un plan de acción para minimizar la exposición al riesgo relacionado a TI generando un listado de actividades a seguir y consideraciones básicas a tomar en cuenta para gestionar los riesgos tecnológicos dentro de la PYME.

2.3. Criterios para determinar el nivel de madurez

Para determinar el estado general de la gestión de riesgos, se plantearan una serie de preguntas que representan aspectos fundamentales a cubrir para la gestión de riesgos agrupándolos en diferentes categorías para analizar el nivel de madurez según Risk IT, para lo cual se estarán manejando las siguientes categorías:

2.3.1. Manejo e implementación de estándares

Para determinar una adecuada gestión de riesgos, se evaluará la aplicación de estándares utilizando las categorías definidas en la tabla III.

Tabla III. **Dimensiones de implementación de estándares**

Categoría	Descripción
Control	Se cuenta con procesos, procedimientos y/o mejores prácticas para el seguimiento y control de riesgos
Documentación	Se cuenta con procesos, procedimientos y políticas definidas para generar documentación de la gestión de riesgos
Medición	Se cuenta con procesos, procedimientos, políticas definidas para la medición del desempeño de la gestión de riesgos

Continuación de la tabla III.

Mejora continua	Se cuenta con procesos, procedimientos y políticas definidas para gestionar la mejora continua en la gestión de riesgos

Fuente: elaboración propia.

2.3.2. Dominios del Framework Risk IT

Alineado al Framework Risk IT, se evaluará la aplicación de los dominios definidos en el marco clasificándolo según las categorías definidas en la tabla IV.

Tabla IV. **Dominios del Framework Risk IT para evaluar el nivel de madurez**

Dominio	Descripción
Gobierno de riesgos	Asegura que las prácticas de gestión de riesgos de TI se encuentran integradas a la empresa, permitiendo asegurar la rentabilidad ajustando el riesgo óptimo
Evaluación de riesgos	El objetivo consiste en asegurar que los riesgos relacionados con TI y las oportunidades, son identificadas, analizadas y se presentan en términos del negocio
Respuesta a riesgos	Garantizar que los temas de riesgo relacionados con TI, las oportunidades y los eventos se abordan de una de manera rentable y de acuerdo con las prioridades del negocio

Fuente: elaboración propia.

2.3.3. Procesos del Framework Risk IT

Alineado al Framework Risk IT, se evaluará la aplicación de los nueve procesos definidos en el marco clasificándolo según las categorías definidas en la tabla V.

Tabla V. **Procesos del Framework Risk IT para evaluar el nivel de madurez**

Proceso	Descripción
Establecer y mantener una visión común de riesgos	Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la empresa de TI relacionados con la pérdida de liderazgo y la tolerancia subjetiva de ella
Integración con ERM	Integrar la estrategia y las operaciones de gestión de riesgos de TI con las decisiones estratégicas de riesgo de negocio que se han tomado a nivel de empresa
Toma de decisiones de negocio conscientes de los riesgos	Asegurar que las decisiones de la organización toman en cuenta la amplia gama de oportunidades y consecuencias generadas de la dependencia de la TI, para el éxito
Recolección de datos	Identificar los datos pertinentes para hacer viable la identificación de riesgos de TI relacionados, el análisis y presentación de informes
Análisis de riesgos	Desarrollar información útil para apoyar las decisiones de riesgo que tenga en cuenta la importancia de factores de riesgo de negocios

Continuación de la tabla V.

Mantenimiento del perfil de riesgos	Mantener actualizado el inventario completo de los riesgos conocidos y los atributos (por ejemplo, que se espera, la frecuencia de impacto potencial, disposición), los recursos, las capacidades y los controles como se entiende en el contexto de los productos empresariales, servicios y procesos
Articular riesgos	Garantizar que la información sobre el estado real de las exposiciones y las oportunidades relacionadas con TI se pone a disposición en forma oportuna y a las personas adecuadas para una respuesta adecuada
Gestionar el riesgo	Garantizar que las medidas para aprovechar las oportunidades estratégicas y reducir los riesgos a un nivel aceptable se gestionan como un portafolio
Reaccionar a acontecimientos	Asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con la TI se activan de forma oportuna y eficaz

Fuente: elaboración propia.

2.3.4. Actividades gestión de riesgos Framework Risk IT

Las categorías definidas agruparan una serie de interrogantes que conformaran la encuesta de evaluación del nivel de madurez de la PYME, las cuales buscan determinar el nivel de cumplimiento de las actividades de gestión de riesgos de TI definidos en el marco de referencia de RISK IT, cuyas actividades se listan en la tabla VI.

Tabla VI. **Actividades del Framework Risk IT para evaluar el nivel de madurez**

ID	Actividad	Proceso	Dominio
RG1.1	Realiza evaluaciones de riesgo de TI en toda la empresa	Establecer y mantener una visión del riesgo común	Gobierno de riesgos
RG1.2	Proponer los umbrales de tolerancia de riesgo de TI	Establecer y mantener una visión del riesgo común	Gobierno de riesgos
RG1.3	Aprobar la tolerancia al riesgo	Establecer y mantener una visión del riesgo común	Gobierno de riesgos
RG1.4	Alinear la política de riesgos de TI	Establecer y mantener una visión del riesgo común	Gobierno de riesgos
RG1.5	Promover la cultura consciente de los riesgos de TI	Establecer y mantener una visión del riesgo común	Gobierno de riesgos
RG1.6	Promover una comunicación efectiva de los riesgos de TI	Establecer y mantener una visión del riesgo común	Gobierno de riesgos
RG2.1	Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa	Integrar con ERM	Gobierno de riesgos
RG2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	Integrar con ERM	Gobierno de riesgos

Continuación de la tabla VI.

RG2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	Integrar con ERM	Gobierno de riesgos
RG2.4	Proporcionar recursos adecuados para la gestión de riesgos	Integrar con ERM	Gobierno de riesgos
RG2.5	Garantizar el aseguramiento independiente sobre la gestión de riesgos	Integrar con ERM	Gobierno de riesgos
RG3.1	Obtener ganancia de la gestión de compra para el enfoque de análisis de riesgos	Tomar decisiones conscientes de los riesgos del negocio	Gobierno de riesgos
RG3.2	Aprobar los resultados del análisis de riesgo	Tomar decisiones conscientes de los riesgos del negocio	Gobierno de riesgos
RG3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	Tomar decisiones conscientes de los riesgos del negocio	Gobierno de riesgos
RG3.4	Aceptar el riesgo de TI	Tomar decisiones conscientes de los riesgos del negocio	Gobierno de riesgos
RG3.5	Priorizar actividades de respuesta a los riesgos de TI	Tomar decisiones conscientes de los riesgos del negocio	Gobierno de riesgos
RE1.1	Establecer y mantener un modelo para la recolección de datos	Recopilar datos	Evaluación de riesgos

Continuación de la tabla VI.

RE1.2	Recopilar datos sobre el entorno externo	Recopilar datos	Evaluación de riesgos
RE1.3	Recopilar datos sobre eventos de riesgo	Recopilar datos	Evaluación de riesgos
RE1.4	Identificar factores de riesgo	Recopilar datos	Evaluación de riesgos
RE2.1	Definir el alcance del análisis de riesgos	Analizar los riesgos	Evaluación de riesgos
RE2.2	Estimar los riesgos de TI	Analizar los riesgos	Evaluación de riesgos
RE2.3	Identificar las opciones de respuesta de riesgo	Analizar los riesgos	Evaluación de riesgos
RE2.4	Realizar una revisión de pares de los resultados de análisis de riesgos de TI	Analizar los riesgos	Evaluación de riesgos
RE3.1	Mapear los recursos de TI para procesos de negocio	Mantener el perfil de riesgo	Evaluación de riesgos
RE3.2	Determinar la criticidad de negocio de los recursos de TI	Mantener el perfil de riesgo	Evaluación de riesgos
RE3.3	Entender las capacidades de TI	Mantener el perfil de riesgo	Evaluación de riesgos
RE3.4	Actualizar los componentes de los escenario de riesgos de TI	Mantener el perfil de riesgo	Evaluación de riesgos
RE3.5	Mantener el registro de los riesgos de TI y el mapa de riesgos de TI	Mantener el perfil de riesgo	Evaluación de riesgos

Continuación de la tabla VI.

RE3.6	Diseñar y comunicar los indicadores de riesgo de TI	Mantener el perfil de riesgo	Evaluación de riesgos
RR1.1	Informar los resultados de análisis de riesgos de TI	Articular riesgos	Respuesta de riesgos
RR1.2	Reportar las actividades de gestión de riesgos de TI y el estado de cumplimiento	Articular riesgos	Respuesta de riesgos
RR1.3	Interpretar los resultados de la evaluación independiente de TI	Articular riesgos	Respuesta de riesgos
RR1.4	Identificar las oportunidades relacionadas con TI	Articular riesgos	Respuesta de riesgos
RR2.1	Controles del inventario	Manejar los riesgos	Respuesta de riesgos
RR2.2	Supervisar la alineación operacional de los umbrales de tolerancia al riesgo	Manejar los riesgos	Respuesta de riesgos
RR2.3	Responder a la exposición al riesgo descubierto y la oportunidad	Manejar los riesgos	Respuesta de riesgos
RR2.4	Implementar los controles	Manejar los riesgos	Respuesta de riesgos
RR2.5	Informar el progreso del plan de acción de riesgos de TI	Manejar los riesgos	Respuesta de riesgos
RR3.1	Mantener los planes de respuesta a incidentes	Reaccionar a acontecimientos	Respuesta de riesgos
RR3.2	Supervisión de riesgos de TI	Reaccionar a acontecimientos	Respuesta de riesgos

Continuación de la tabla VI.

RR3.3	Iniciar planes de respuesta a incidentes	Reaccionar a acontecimientos	Respuesta de riesgos
RR3.4	Comunicar las lecciones aprendidas de eventos de riesgo	Reaccionar a acontecimientos	Respuesta de riesgos

Fuente: elaboración propia.

2.3.5. Categorías generales gestión de riesgos de TI

La evaluación incluye preguntas generales con las cuales se buscará establecer la situación actual de la PYME en relación a la gestión de riesgos desde un punto de vista macro, según las categorías definidas en la tabla VII.

Tabla VII. **Categorías para evaluar la gestión de riesgos de TI**

Categoría	Descripción
Modelos, planes y procedimientos definidos	Modelos, planes y procedimientos para la identificación de riesgos y respuesta al riesgo tecnológico
Gestión de comunicación	Comunicación de la información, procedimientos, planes y acciones definidas relacionadas con la gestión de riesgos de TI, a las personas interesadas y responsables de los procesos
Apetito al riesgo	Establecer umbrales de exposición al riesgo, identificación de nuevas oportunidades y riesgos positivos que generen beneficios y permitan apalancar el cumplimiento de los objetivos estratégicos

Continuación de la tabla VII.

Reportes y estadísticas	Elaboración de informes de gestión y análisis de riesgos que permitan evaluar y mejorar los controles de riesgos definidos para garantizar el monitoreo constante y ciclo de mejora continua
Seguimiento y control	Análisis de desempeño y supervisión de los controles para garantizar que las acciones tomadas para mitigar el riesgo, cumplen con los objetivos definidos por el comité responsable de la gestión de riesgos y permiten tomar decisiones oportunas para mejorar y optimizar los controles implementados
Responsabilidad	Definición de roles y responsabilidades de las personas interesadas para gestionar los riesgos de TI por medio de lineamientos claros, manuales de puesto y funciones especificas orientadas a la mitigación del riesgo tecnológico
Alineamiento	Alineamiento a objetivos estratégicos brindando un lenguaje común e integración con ERM que permita que la gestión de riesgos tecnológicos se encuentre orientado y priorizado de acuerdo a los objetivos estratégicos del negocio

Fuente: elaboración propia.

3. EVALUACIÓN DEL NIVEL DE MADUREZ DE UNA PYME

Establecer el nivel de madurez de la PYME permitirá conocer la situación actual de la empresa para gestionar el riesgo tecnológico, lo cual será la base para definir el plan de acción que permita minimizar la exposición al riesgo. Para determinar el nivel de madurez se procederá a definir una encuesta que cubrirá los criterios definidos en el apartado 2.3, y posteriormente se analizaran los resultados para determinar el nivel de madurez por cada uno de los dominios del Framework Risk IT.

3.1. Definición de encuesta

Definidos los criterios de evaluación, procedemos a diseñar el set de preguntas a realizar para determinar a nivel general la gestión de riesgos dentro de la PYME, la implementación de estándares y el nivel de madurez de acuerdo a los 3 dominios, 9 procesos y 43 actividades definidas por el Framework Risk IT. En el apéndice se muestra la encuesta que se realizo a una PYME por medio de una entrevista, con la cual se diagnosticó el nivel de madurez y así determinar brechas a cerrar por medio del plan de acción.

La evaluación se compone de dos secciones, la primera incluye 8 preguntas generales para determinar la gestión de riesgos que realiza la PYME y la segunda sección se conforma de 209 preguntas que se evalúan de acuerdo a la frecuencia con que la PYME realiza las actividades relacionadas a la gestión de riesgos según el Framework Risk IT, que a su vez son utilizadas para determinar el nivel de madurez y control del la PYME, agrupando las respuestas de acuerdo a los criterios descritos en el apartado 2.3.

Para obtener una visión más clara de la distribución de preguntas por cada una de las categorías establecidas para el análisis se recomienda ver el anexo “A”, en donde se listan las preguntas asignadas para cada uno de los diferentes criterios evaluados.

3.2. Interpretación de resultados

Para el estudio realizado, se evaluó la empresa Almacenes Japon, la cual es una empresa que opera en el país de Guatemala desde el año 2001, ofreciendo a las familias guatemaltecas una serie de productos que incluyen línea blanca, electrodomésticos, muebles, electrónicos, tecnología, entre otros; cuyos productos pueden adquirirse en cualquiera de sus 18 tiendas por medio de diferentes formas de compra que ofrecen: crédito, efectivo, tarjeta de crédito/debito o a través del crédito de otras instituciones, esto según la conveniencia de los guatemaltecos.

La empresa cuenta actualmente con un sistema de gestión de ventas y créditos en línea que intercomunica las sucursales, teniendo entre 100 y 500 usuarios que utilizan el sistema; a dichos usuarios se da soporte por parte del equipo responsable de tecnología.

En el apéndice encontrará la encuesta con la cual se realizó la evaluación de la frecuencia de ejecución de actividades relacionadas a la gestión de riesgos, así como las respuestas dadas por la empresa evaluada.

3.2.1. Aspectos generales de evaluación de riesgos

Durante la evaluación se determinó que la PYME evaluada, administra los riesgos relacionados al negocio y relacionados a tecnología por medio de una

metodología propietaria definida por la dirección de tecnología, acompañada de políticas, procedimientos y normativas para gestionar los recursos y servicios que brinda TI; asimismo, se determinó que la empresa aprovecha la tecnología para el cumplimiento de sus objetivos estratégicos y que en caso de detección de riesgos se sabe que acciones deben seguirse para reaccionar ante los riesgos, sin embargo, las acciones a seguir no se encuentran documentadas por lo cual, dependen del conocimiento del personal a cargo de la administración y gestión de recursos y servicios tecnológicos.

Se observa que no se cuenta con un portafolio, un inventario, un perfil de riesgos ni una matriz de riesgos para gestionar los riesgos asociados a TI y tampoco se cuenta con controles que permitan monitorear y tener control de los riesgos a los cuales la empresa se encuentra expuesta.

Los resultados evidencian que se conoce de los riesgos asociados a TI sin embargo se lleva un control manual no documentado ni con planes definidos para minimizar la exposición a riesgos, lo cual incrementa el riesgo e impacto sobre el negocio al momento de materializarse alguno de estos riesgos. Para analizar a mayor profundidad la situación actual de la empresa en relación a la gestión de riesgos, en las siguientes secciones se evalúan los resultados basados en la adopción de estándares y actividades correspondientes a procesos y dominios definidos por el Framework Risk IT de ISACA.

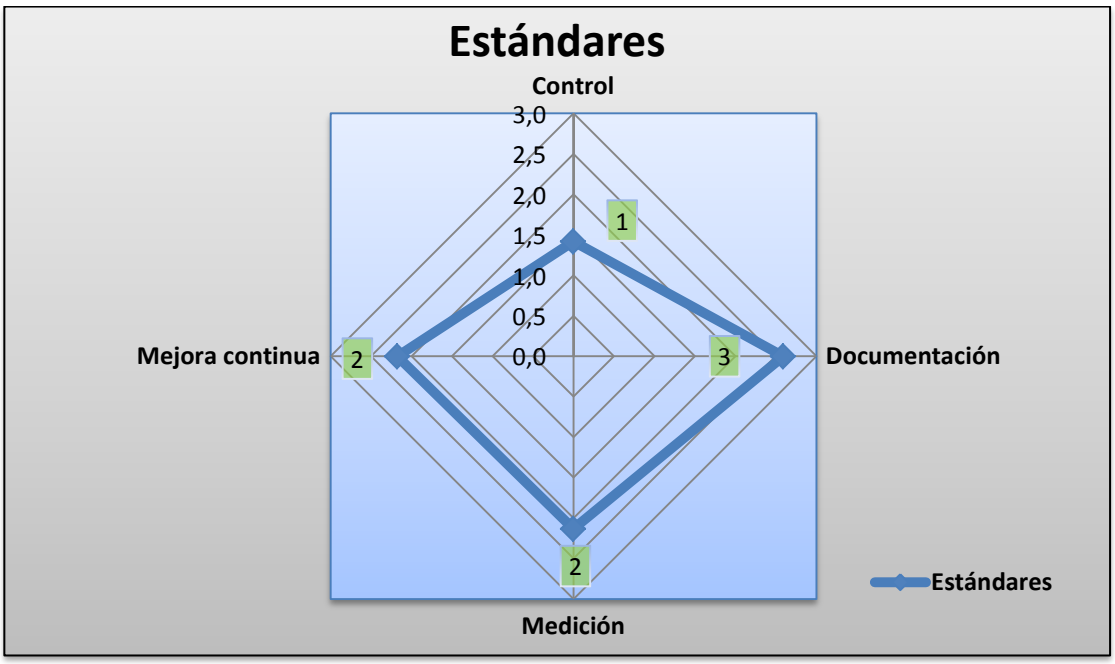
3.2.2. Aplicación de estándares para la gestión de riesgos tecnológicos

En esta sección se observa la implementación de estándares que realiza la PYME evaluada para la gestión del riesgo informático, agrupando los criterios

de evaluación en estándares de control, documentación, medición y mejora continua. La puntuación se puede observar en el anexo “B.1”.

La figura 10 muestra que rara vez son aplicados estándares de control ya que no se analiza el origen de los riesgos ni se coordinan actividades de control de riesgos, no son monitoreados y tampoco se supervisa el cumplimiento de una política de riesgos.

Figura 10. **Frecuencia de aplicación de estándares para la gestión de riesgos de TI**



Fuente: elaboración propia.

En relación a documentación de riesgos de TI, se observa que frecuentemente se aplican estándares ya que se documentan procesos y procedimientos para la gestión de riesgos tomando en consideración el apetito

al riesgo de la empresa dentro de la política de riesgos, son identificados los riesgos inherentes a los objetivos estratégicos, existe una comunicación de los riesgos aceptados y se documentan las respuestas a dar ante riesgos así como el análisis realizado de riesgos; sin embargo, no se definen planes de acción para minimizar los riesgos, no se cuenta con una matriz de riesgos que evidencie la criticidad ante el negocio y no son definidas las áreas clave de gestión de riesgos así como los indicadores para medir el desempeño.

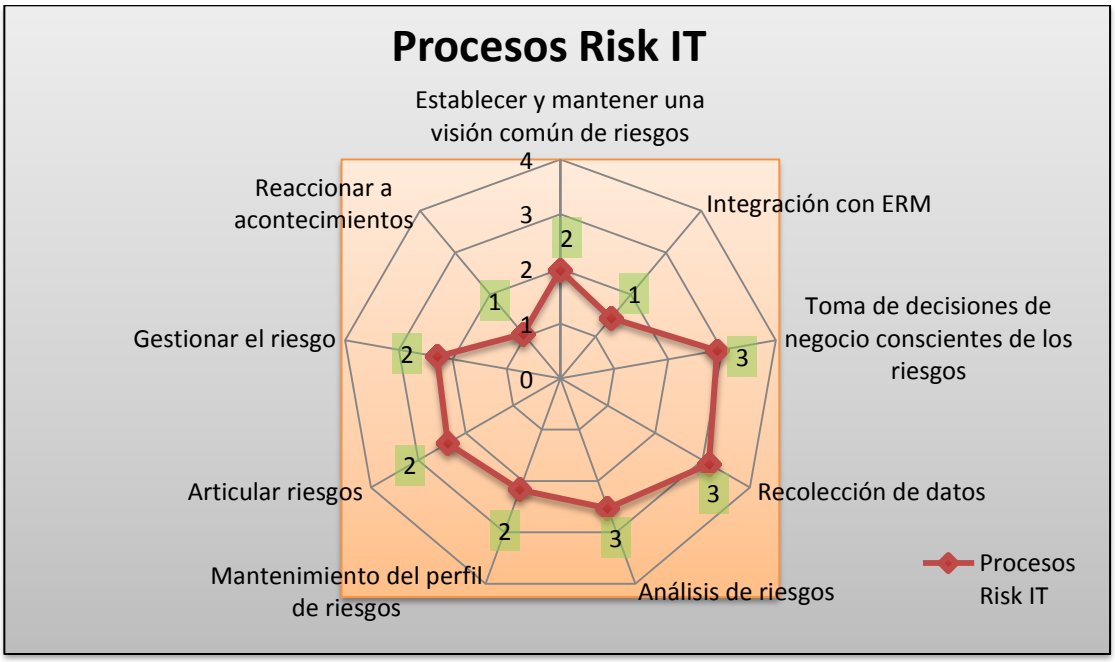
En relación a la aplicación de estándares para la medición, se observa que en ocasiones se realiza debido a que los incidentes no son clasificados ni cuantificados, raras veces se definen métricas e indicadores para medir el riesgo y raras veces estos son supervisados; sin embargo, se considera que se tiene un avance ya que siempre son realizadas pruebas piloto para garantizar el funcionamiento de aplicaciones contra el diseño realizado, y se definen las expectativas para controles a implementar sobre puntos donde se espera que se extenderán los riesgos de tal forma que puedan tener una visibilidad que les permita reaccionar ante estos.

En relación a la aplicación de estándares para mejora continua se observa que estos son aplicados en ocasiones ya que no se realizan ensayos de escenarios para áreas no cubiertas por la política de riesgos, rara vez se evalúan eventos de riesgos ocurridos en el pasado, no se identifica la causa raíz de incidentes y no se evalúa la eficacia de acciones tomadas con anterioridad; tampoco se actualiza el mapa de riesgos, niveles de tolerancia, indicadores de desempeño y controles ni se da mantenimiento a la documentación que se genera.

3.2.3. Ejecución de procesos de gestión de riesgos tecnológicos según Risk IT

En esta sección se observa la aplicación de los nueve procesos para la gestión de riesgos definidos por el Framework Risk IT para la gestión de riesgos por parte de la PYME evaluada. Para el efecto se evalúa el cumplimiento de actividades específicas de los procesos del marco de referencia que buscan: establecer y mantener una visión común de riesgos, integración con ERM, toma de decisiones de negocio conscientes de los riesgos, recolección de datos para análisis de riesgos, análisis de riesgos, mantenimiento del perfil de riesgos, articulación de riesgos, gestión del riesgo y reacción a incidentes de riesgos.

Figura 11. **Frecuencia de ejecución de actividades de los procesos del Framework Risk IT**



Fuente: elaboración propia.

La puntuación obtenida se puede observar en el anexo “B.2” y en el anexo “C”, donde se muestra la frecuencia con la cual la PYME ejecuta las actividades para gestión de riesgos de TI definidas en el Framework Risk IT.

De los resultados obtenidos, se observa que la PYME raras veces logra establecer y mantener una visión común de riesgo debido a que solo en algunas ocasiones logra cumplir con actividades que permiten evaluar los riesgos de TI en la empresa, algunas veces logra proponer umbrales de tolerancia para dichos riesgos y aprueban los niveles de tolerancias, a veces se promueve una comunicación efectiva de los riesgos de TI, mientras que rara vez se promueve una cultura de consciencia de riesgos y frecuentemente se alinea la política de riesgos de TI con la empresa.

En relación a la integración con ERM, se observa que raras veces se realizan actividades para que la gestión de riesgos de TI se encuentre alineada con la gestión de riesgos del negocio; esto se debe a que es raro que se coordinen los riesgos de TI con los riesgos del negocio, que se adapten los riesgos de TI a prácticas para la gestión de riesgos, que se proporcionen recursos adecuado para la gestión de riesgos y que se provea aseguramiento independiente sobre la gestión de riesgos de TI.

En relación a la toma de decisiones del negocio conscientes de los riesgos de TI a los cuales se encuentra expuesta la PYME, se observa que frecuentemente se realizan actividades para asegurar que las decisiones de la organización toman en cuenta la amplia gama de oportunidades y consecuencias que se generan por la dependencia que se tiene en TI, esto se debe a que frecuentemente se aprueban resultados de análisis de riesgos de TI, se incorporan consideraciones de riesgos de TI a la toma de decisiones estratégicas del negocio, se aceptan riesgos de TI y se priorizan actividades de

respuesta a los riesgos de TI, sin embargo, en su mayoría queda a cargo de la dirección de TI.

En relación a la recolección de información y datos para el análisis e identificación de riesgos, se observa que la PYME evaluada realiza frecuentemente actividades que permitan establecer y mantener un modelo para la recolección de datos; siempre se recolectan datos sobre el entorno operativo y de eventos de riesgos; y, a veces se logran identificar factores de riesgo relacionados a TI.

En relación a procesos de análisis de riesgos, se observa que la PYME frecuentemente analiza los riesgos a los cuales está expuesta, en ocasiones se define el alcance del análisis de riesgo y se estiman los riesgos de TI, siempre se identifican las opciones que se tienen para dar respuesta a riesgos de TI y frecuentemente se realizan evaluaciones por pares del análisis de riesgos de TI.

Con respecto al proceso de mantenimiento del perfil de riesgos, se observa que la PYME evaluada algunas veces cumple con dicho proceso dado que solo algunas veces se actualizan componentes de escenarios de riesgo para su análisis, se da mantenimiento al perfil y mapa de riesgos de TI y, se definen indicadores de riesgos de TI, sin embargo frecuentemente se mapean los recursos de TI contra los recursos de negocio y se determina la criticidad que tienen dichos recursos en el negocio para entender las capacidades de TI.

En relación al proceso de respuesta a los riesgos de TI para Articular los riesgos, se observa que solo algunas veces se logra que la información sobre el estado real de la exposición y oportunidades relacionadas a TI se ponga a disposición de forma oportuna y a las personas adecuadas para obtener una respuesta adecuada. Esto se debe a que solamente algunas veces se

comunican los resultados del análisis de riesgo, se informa de actividades de gestión de riesgos de TI y se comunica el estado del cumplimiento de dichas actividades, así como solo algunas veces se interpretan los resultados de evaluaciones independientes de TI; sin embargo, se observa que frecuentemente se identifican oportunidades relacionadas con TI para beneficio del negocio.

En relación a los procesos específicos para gestionar el riesgo que garantizan las medidas para aprovechas oportunidades estratégicas y reducir los riesgos a un nivel aceptable para la empresa, se observa que la PYME algunas veces logra gestionar de forma adecuada los riesgos de TI, raras veces se monitorea la alineación operacional con los umbrales de tolerancia de riesgos, algunas veces se realizan actividades para mantener un inventario de controles de riesgos y algunas veces se informa del progreso del plan de acción de riesgos de TI; asimismo, se observa que frecuentemente se da respuesta a riesgos a los cuales está expuesta la PYME así como se toman en consideración las oportunidades que se descubren.

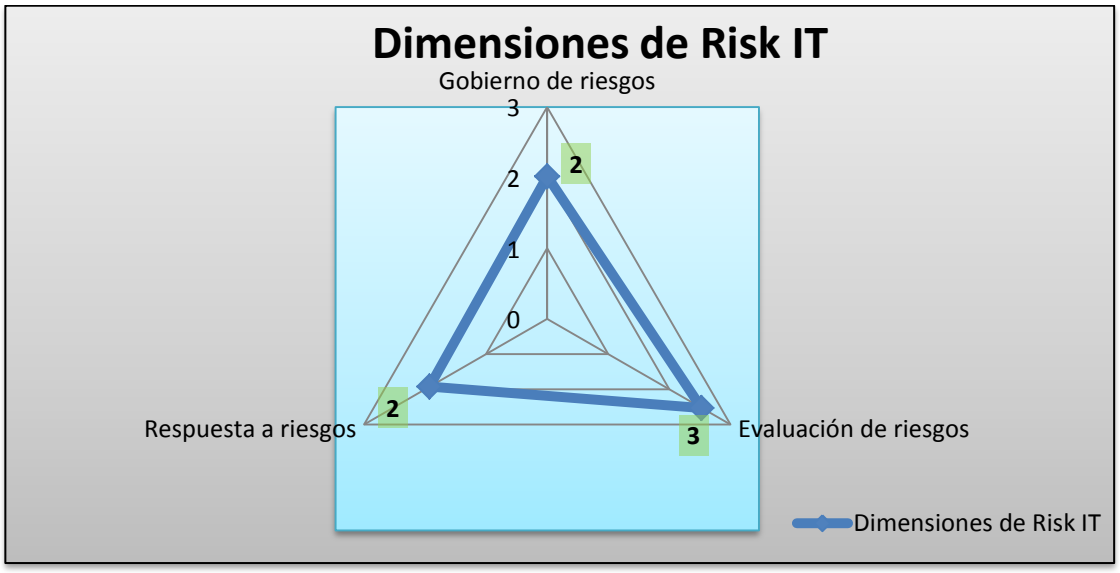
Por último, se observa que para el proceso de reacción a acontecimientos de riesgo o incidentes, la PYME raras veces logra responder de forma inmediata a los riesgos y limitar la magnitud de pérdida a acontecimientos relacionados a TI por medio de medidas que se activen de forma oportuna y eficaz; esto se debe a que raras veces se realizan actividades que den mantenimiento a planes de respuesta a incidentes, supervisión de riesgos, ejecución de planes de respuesta y comunicación de lecciones aprendidas sobre eventos de riesgos materializados o vividos por la PYME.

3.2.4. Cumplimiento de dimensiones de gestión de riesgos tecnológicos según Risk IT

En esta sección se determina la aplicación de las tres dimensiones definidas por el Framework Risk IT para la gestión de riesgos por parte de la PYME evaluada. Para el efecto se analiza el cumplimiento de actividades para la gestión del gobierno de riesgos, evaluación de riesgos y respuesta al riesgo. La puntuación obtenida se puede observar en el anexo “B.3”.

En la figura 12, se observa que la PYME ejecuta algunas veces las actividades definidas en el Framework Risk IT para el gobierno de riesgos mediante las cuales se asegura que las prácticas de gestión de riesgos de TI se encuentran integradas a la empresa permitiendo garantizar la rentabilidad ajustando los riesgos de tal forma que estos sean óptimos para la empresa.

Figura 12. **Frecuencia de ejecución de actividades de los dominios del Framework Risk IT**



Fuente: elaboración propia.

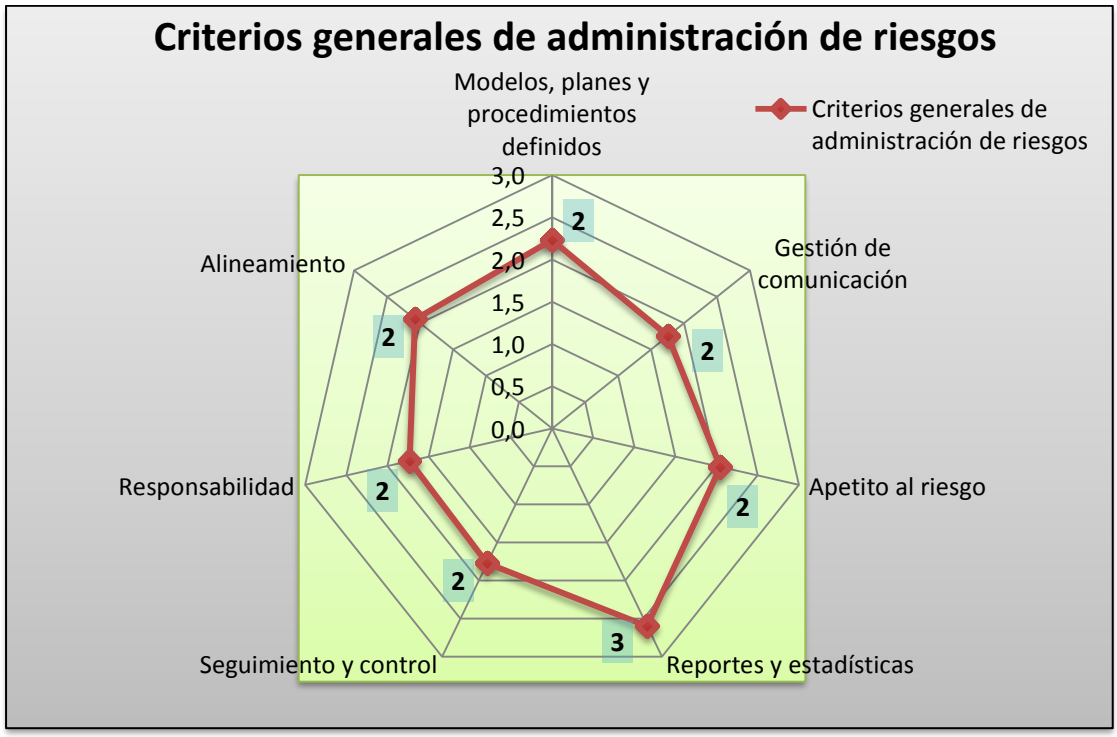
En relación a la evaluación de riesgos, se observa que frecuentemente se evalúan los riesgos a los cuales se encuentra expuesta la organización en su mayoría para identificar la razón u origen del riesgo y establecer acciones a seguir para su mitigación sin embargo rara vez estos son comunicados y se les da seguimiento para mejorar los resultados de la organización.

A pesar que la PYME evalúa los riesgos frecuentemente, la respuesta a los mismos se realiza algunas veces por lo tanto la empresa no garantiza que las oportunidades identificadas resultantes de la evaluación de riesgos de TI se aborden de una manera rentable para la empresa y según las prioridades del negocio, con lo cual se da una respuesta tardía a los riesgos identificados exponiendo a la empresa a considerables pérdidas si alguno de los riesgos se llegara a materializar.

3.2.5. Cumplimiento de criterios generales de administración de riesgos

En esta sección se analiza el cumplimiento de criterios generales para la gestión de riesgos por parte de la PYME evaluada. Para el efecto se analiza si la empresa cuenta con: modelos, planes y procedimientos definidos para la gestión de riesgos, si se gestiona la comunicación de riesgos, si se define el apetito al riesgo de la empresa, si se generan reportes y estadísticas relacionadas a la gestión de riesgos, si se da seguimiento y control a los riesgos, si son definidas las responsabilidades para la gestión de riesgos y, si la gestión de riesgos se encuentra alineada a los objetivos estratégicos e integrada con ERM. La puntuación obtenida se puede observar en el anexo “B.4”.

Figura 13. **Aplicación de criterios generales para la gestión de riesgos**



Fuente: elaboración propia.

Durante la evaluación se identificó que la PYME evaluada, algunas veces cumple con la ejecución de actividades para la gestión de riesgos, detectando que solamente la generación de reportes y estadísticas es la que se realiza de forma frecuente; sin embargo, se observa que la empresa no cuenca con modelos y planes claros que les permita identificar de forma oportuna los riesgos a los cuales se encuentran expuestos y tampoco los resultados de evaluaciones de riesgos son aprovechados para incrementar el apetito al riesgo ya que estos son atendidos para mitigar riesgos pasados y no para aprovechar oportunidades o implementar indicadores para ajustar un modelo de gestión de riesgos para escenarios futuros.

Debido a que no se comunican de forma adecuada los riesgos, estos no se toman en consideración de forma oportuna en la toma de decisiones del negocio, no se logra tener un alineamiento a la estrategia ni a la gestión de riesgos empresariales y, tampoco pueden definirse responsabilidades para gestionar el riesgo o dar respuestas oportunas si estos se llegan a materializar.

Asimismo, tampoco se da seguimiento y control a riesgos lo cual se evidencia al no contar con controles adecuados para identificar y detectar cuando un riesgo excede los umbrales de tolerancia definidos por el negocio lo cual a su vez, al no darles seguimiento no permite que la empresa tome en consideración los escenarios vividos para ajustar el apetito al riesgo y poder aprovechar oportunidades que den apalancamiento al negocio o mitiguen la exposición a riesgos relacionados a TI.

3.3. Nivel de madurez en la gestión de riesgos de TI

En esta sección se analizan los resultados obtenidos de la encuesta para la PYME evaluada con el objetivo de identificar el nivel de madurez que tiene la misma sobre los tres dominios sobre los cuales se fundamenta el Framework Risk IT para la gestión de riesgos tecnológicos. Como primer punto lo que se observa es que no existe una consciencia de riesgos en la organización que a través de una cultura de riesgos fomente la comunicación y defina responsabilidades con funciones a realizar en respuesta a la materialización de riesgos o para mitigar la exposición a riesgos tecnológicos. A pesar que se tiene conocimiento de la exposición a riesgos, se aplican procesos Ad Hoc y respuestas no documentadas lo cual genera dependencia del personal actual.

3.3.1. Nivel de madurez gobierno de riesgos de TI

Dado que las actividades para este dominio son realizadas algunas veces ya que la media de frecuencias obtenida fue de dos, lo cual corresponde a una frecuencia de ejecución de “a veces” y, considerando los resultados de la evaluación, se considera que la PYME tiene un nivel de madurez Ad Hoc de acuerdo a los niveles definidos por COBIT ya que se realizan acciones para mitigar el riesgo reconociendo las necesidades de reaccionar antes estos, sin embargo estos son limitados y no atendidos de raíz, se sabe que hacer sin embargo depende de la experiencia de cada responsable y los procedimientos no se encuentran documentados.

Desde el punto de vista del Framework Risk IT, el nivel de madurez se encuentra entre el nivel “inicial” y “repetible” ya que se tiene consciencia de la necesidad de atender los riesgos sin embargo, la atención de los mismos se centra en atenderlos técnicamente sin buscar valor sobre los mismos, tampoco se cuenta con roles o responsables para realizar funciones que permitan atender el riesgo ni se cuenta responsables por área para tomar decisiones. Se cuenta con niveles de tolerancia definidos a nivel local y no estandarizados para la empresa. No se da orientación a la junta directiva de los riesgos y tampoco existe una retroalimentación de los mismos, así como de la atención de estos para mitigar la exposición a los riesgos.

En el nivel inicial, la responsable de la gestión de problemas relacionados a TI, se encuentra a cargo del área de tecnología, las inversiones son enfocadas según exigencias externas y en el nivel repetible se enfocan según necesidades del negocio o funcionales las cuales no siguen un alineamiento a los niveles de tolerancia y planes estratégicos de la organización. Por otro lado, en el nivel en el cual se encuentra la PYME, la retroalimentación de informes se

dirige a la gestión de TI local, lo cual no permite tomar en consideración los hallazgos u oportunidades en planes estratégicos para maximizar los resultados a obtener del plan estratégico.

En relación a la definición de políticas, normas y procedimientos, la PYME se encuentra en un nivel “repetible” esto debido a que se cuentan con procedimientos definidos sin embargo estos no se encuentran alineados al apetito al riesgo del negocio; por otro lado, a nivel de experiencia y habilidades el nivel de madurez es “repetible” dado que no se cuenta con requisitos de formación y en su mayoría son orientadas a acontecimientos e incidentes ocurridos o por medio de formación informal.

3.3.2. Nivel de madurez evaluación de riesgos de TI

De acuerdo a los resultados de la evaluación realizada a la PYME se observa que la empresa realiza frecuentemente actividades para la evaluación del riesgo y su nivel de madurez en la evaluación de riesgos es “inicial”, ya que se sabe que debe identificarse el riesgo y el análisis de riesgos de TI se realiza sobre una base ad hoc. En este nivel la comunicación es mínima a personas responsables de la toma de decisiones del negocio y de riesgos del negocio.

En este nivel, la identificación de riesgos no es realizada en el contexto de actividades comerciales u operativas alineadas a umbrales de tolerancia sino basados en los peores escenarios los cuales a su vez son utilizados para definir las acciones a realizar para mitigar los riesgos que se han materializado. A su vez, las políticas y procedimientos para la evaluación de riesgos, sigue actividades para recopilar datos y analizar la información que son definidos por los responsables de TI o son Ad Hoc y las evaluaciones de riesgos no incluyen todos los componentes de riesgos.

Tampoco se cuenta con gestores de riesgos de TI por lo cual las actividades de gestión de riesgos existen sobre una base Ad Hoc las cuales no se desarrollan de forma activa y el personal de TI no cuenta con conocimientos ni habilidades para determinar relaciones o congruencia con el negocio de los factores de riesgo.

3.3.3. Nivel de madurez respuesta a riesgos de TI

De acuerdo a los resultados obtenidos por medio de la encuesta, se determino que la frecuencia de ejecución de actividades para dar respuesta a los riesgos tecnológicos se encuentra en el segundo nivel de madurez debido a que “a veces” se realizan las actividades definidas en el Framework Risk IT, lo cual evidencia que la PYME reconoce la necesidad de responder ante los riesgos a los cuales se encuentra expuesta, sin embargo, solamente se enfoca en evitar los riesgos, tampoco se refleja una cultura que fomente la consciencia de gestionar los riesgos en cada área ni se definen acciones concretas a realizar por roles específicos para mitigar los riesgos tecnológicos, si estos llegara a materializarse.

En este nivel, se identifican posibles escenarios que pueden afectar la operación sin embargo no se plantean respuestas a riesgos específicos y tampoco se cuenta con controles específicos que permitan garantizar el cumplimiento en la mitigación de riesgos o indicadores que reflejen la eficacia de acciones definidas para mitigar riesgos tecnológicos. Los riesgos identificados o tratados, tampoco son comunicados al momento de materializarse ni se retroalimentan las acciones tomadas para dar respuesta al riesgo; no existen responsabilidades definidas para garantizar que las medidas tomadas para responder ante el riesgo son eficaces y que estas se encuentran alineadas a los niveles de tolerancia definidos por el negocio.

Por lo regular, los controles se implementan de forma reactiva, es decir, se toman acciones hasta que la empresa se ve afectada por un riesgo que llega a materializarse; no se implementan controles de forma proactiva por lo cual no son oportunos y tampoco se implementan controles de riesgos no conocidos que posiblemente expongan las operaciones del negocio. A su vez, las respuestas que se dan para mitigar la exposición al riesgo, no se comparan con las prioridades del negocio y, en su mayoría los lineamientos definidos en políticas, procedimientos o normas para la gestión de riesgos se basan en requisitos de cumplimiento, son definidos para gestionar riesgos particulares y no son estandarizados en las diferentes áreas del negocio.

En este nivel, se implementan controles a la medida los cuales no se relacionan al riesgo ni el impacto, tampoco se considera la efectividad que estos tienen o beneficio que otorgaran al negocio en relación coste/beneficio para determinar la viabilidad de implementación según los resultados a obtener contra el costo de inversión para su implementación.

El no considerar el costo/beneficio de implementación de controles, a nivel gestión de riesgos por parte de TI y de acuerdo a los recursos asignados puede ocasionar que la empresa acepte riesgos fuera de los umbrales de tolerancia y que se gestione un portafolio de proyectos para minimizar el impacto de escenarios de riesgo, sin considerar la crisis o criticidad de acuerdo al impacto que representen los riesgos identificados para la organización y estos fuera de sintonía o desalineando a los planes estratégicos de le empresa, pudiendo incurrir en costos innecesarios y afectar el cumplimiento de objetivos estratégicos.

4. PLAN DE ACCIÓN PARA MINIMIZAR EL RIESGO TECNOLÓGICO BASADO EN RISK IT

Considerando los resultados obtenidos por medio de la encuesta en donde se visualiza que la PYME tiene conocimientos de los riesgos existentes y se realizan gestiones para responder a incidentes y, a su vez reflejan que no existe una política, metodología o procesos definidos para gestionar los riesgos, tampoco son alineados a los objetivos del negocio y no se documentan los procesos, se considera que él nivel de madurez para la gestión de riesgos es el “inicial”, esto se debe a que se conoce la exposición de riesgos y se realizan acciones para mitigarlos sin embargo estas de forma reactiva.

Debido a la situación actual, se propone el siguiente plan de acción alineado al Framework Risk IT para minimizar la exposición al riesgo tecnológico por parte de la PYME evaluada, mediante el cual se pretende cumplir con una gestión integral de riesgos, identificación de riesgos, medición, monitoreo, control y respuesta al riesgo, y retroalimentación por medio de informes de evaluación de riesgos.

En pro de minimizar la exposición al riesgo y alineado al cumplimiento de la gestión de riesgos definida en el apartado 1.3, según la figura 5 de dicha sección, se plantea la ejecución de las siguientes actividades para minimizar la exposición a riesgos tecnológicos a los cuales se encuentra expuesta la PYME.

4.1. Organización de la gestión de riesgos

Acá se pondrá en orden la gestión de riesgos estableciendo criterios generales que deben realizarse para poder iniciar con la implantación de la cultura de gestión de riesgos basada en el Framework Risk IT, para el efecto primero se debe trabajar en definir los criterios iniciales para la gestión de riesgos, identificar las capacidades y procesos actuales del negocio, definir el nivel de madurez esperado, establecer los roles y responsabilidades para la gestión de riesgos.

4.1.1. Alinear la estrategia del negocio a los objetivos de TI

La dirección de tecnología debe tener conocimiento de los objetivos estratégicos del negocio de tal forma que todo plan de trabajo definido por tecnología debe estar orientado a cumplir los planes estratégicos del negocio.

Esta es una gestión del gobierno corporativo que requiere que tecnología sea parte de la toma de decisiones estratégicas y que se tome en consideración su posición en la definición de acciones a realizar para el desarrollo e implementación de proyectos; para lograrlo deben listarse los objetivos del negocio y compararlos con los objetivos de TI, esto permitirá identificar brechas que deben atacarse de forma estratégica. Por ejemplo, si la PYME pretende crear nuevas sucursales de venta, dentro de la estrategia de TI debe incluirse proveer una plataforma que brinde servicios sostenibles y que garantice que los riesgos asociados a TI se administran de forma eficaz, considerando las tendencias actuales de la exposición de la información.

Al incluir los planes de tecnología a los planes estratégicos, se permitirá tener un adecuado control de recursos y priorizar la atención de proyectos

enfocados en las capacidades de TI para la atención del soporte operativo y, la ejecución de proyectos; esta alineación puede requerir esfuerzos adicionales como el gestionar un portafolio de proyectos y un inventario de activos o recursos, sin embargo esto permitirá implementar una gestión de servicios y recursos de TI de forma eficiente, alineada a las expectativas y planes estratégicos del negocio.

4.1.2. Evaluar la capacidad de TI

Es muy importante que se tenga un conocimiento de las capacidades que tiene la organización para gestionar las operaciones, soporte, servicios y proyectos a los cuales tiene dependencia el negocio de TI. De acuerdo a las capacidades de TI se puede determinar el nivel de sofisticación y de complejidad de TI lo cual es una base primordial para determinar el nivel de control que se requiere sobre el cumplimiento de sus operaciones y el posible riesgo al cual puede estar expuesta la organización por la dependencia que tenga en el uso de tecnología.

Para poder determinar el nivel de sofisticación, es necesario que la PYME alimente un inventario de activos, servicios y recursos tecnológicos con los que cuenta, manteniéndolo actualizado y documentado para realizar un adecuado control el cual servirá de base para tomar en consideración la capacidad que tiene el área de TI.

En la revista de ISACA[9] volumen 1 del año 2010, se plantea un modelo para determinar el nivel de sofisticación de TI en una empresa, el cuál toma en

[9] ISACA Journal, Fuente de los profesionales de Gobierno de TI. Revista bimestral que ofrece conocimiento práctico y profesional de temas críticos relacionados a la auditoria de TI, gobierno, seguridad y riesgos. http://www.isaca.org/Journal/Pages/default.aspx

consideración criterios relacionados a la cantidad de servidores, sistemas operativos utilizados, cantidad de estaciones de trabajo, aplicaciones, cantidad de ubicaciones remotas, controles internos sobre información financiera, uso de tecnologías nuevas, emergentes o avanzadas y, cantidad de transacciones realizadas en línea; estos criterios pueden tomarse en consideración para el análisis de las capacidades de TI.

4.1.3. Definir el nivel de madurez deseado

Hasta el momento se tiene identificado que la PYME evaluada se encuentra en un nivel de madurez uno, el cual corresponde a un proceso de gestión de riesgos tecnológicos iniciado pero que no genera valor para la organización. Por lo cual es necesario que se defina el alcance que tendrá a nivel organizacional la gestión de riesgos tecnológicos que debe incluir las diferentes áreas del negocio y procesos que estén expuestos a riesgos tecnológicos.

El nivel de madurez deseado (ver sección 2.1) debe estar alineado a los objetivos estratégicos del negocio tomando en consideración el estado actual y los esfuerzos necesarios para alcanzarlo. Asimismo, deben evaluarse la aplicación de niveles de madurez por área dependiendo del impacto que tengan los riesgos de TI en el cumplimiento de los objetivos de negocio, esto permitirá una mejor gestión y minimizar los costos de implementación.

4.1.4. Definir roles y responsabilidades para la gestión de riesgos

Es importante definir de acuerdo al nivel de madurez deseado, una estructura organizativa para la gestión de riesgos. Esto dependerá de las

capacidades que se tengan en la empresa para asignar recursos dedicados en tiempo completo o parcial a la gestión de riesgos lo cual debe estar apegado a los objetivos estratégicos del negocio. Acá la dirección ejecutiva deberá tener en consideración el apetito al riesgo que se defina ya que mientras mayor sea el nivel de madurez esperado, mayor será la inversión necesaria para implementar la gestión de riesgos tecnológicos.

Adicional a la estructura organizacional que debe establecer los puestos que estarán a cargo, roles y responsabilidades debiendo definir el comité de riesgos que dará seguimiento al cumplimiento de la gestión de riesgos y tomará decisiones relacionadas a dicha gestión. Como mínimo deberá contarse con un oficial de seguridad tecnológica que será la persona que dará seguimiento a la implementación de controles y supervisara el cumplimiento de las actividades definidas para gestionar el riesgo, asimismo será el responsable de la mejora continua de la gestión de riesgos.

De acuerdo a las áreas identificadas que se encuentran expuestas a riesgos tecnológicos, deberán definirse responsables por área para monitorear y dar seguimiento a controles e indicadores implementados para la gestión de riesgos, de tal forma que estos tengan la capacidad de responder a dichos riesgos si se llegaran a exceder los umbrales de tolerancia.

Un entregable principal de esta actividad es el organigrama que define la estructura organizativa del equipo responsable de la gestión de riesgos e incluye los responsables por área, asimismo, deberán proporcionarse los manuales de puesto que definen el objetivo del puesto y sus responsabilidades en la gestión de riesgos.

4.1.5. Identificar del las principales líneas del negocio y procesos prioritarios

Uno de los factores importantes para gestionar adecuadamente los riesgos es realizar una distinción de unidades del negocio, áreas, departamentos o divisiones que generan o se encuentran expuestas a riesgos tecnológicos. Para esto es necesario que se identifiquen las unidades del negocio con sus funciones y valor que dan como parte del servicio que provee la empresa. Cada línea de negocio para el cumplimiento de sus funciones realiza una serie de actividades y procesos que generan servicios o productos que aportan valor a la empresa por lo cual es importante tener claro las funciones que realizan y los procesos que estas ejecutan para dar cumplimiento a sus funciones.

Las líneas del negocio deberán priorizarse ordenándolas de mayor prioridad a menor prioridad, a su vez, deberán listarse los procesos clave del negocio para identificar cuáles son los que tienen dependencia de TI y se encuentran expuestos a riesgos tecnológicos, esta clasificación será de utilidad para definir la estrategia a seguir para gestionar el riesgo y alcanzar el nivel de madurez deseado.

4.2. Definición de políticas, procedimientos y normas de gestión de riesgos

Se deberán definir políticas, procedimientos y normas internas por parte del comité de riesgos asignado para que estas sean implementadas en la organización de tal forma que tanto responsables de la gestión de riesgos como miembros de la organización cumplan los lineamientos estipulados en las mismas. Asimismo, deberá estar a cargo del oficial de seguridad tecnológica,

velar por el cumplimiento de estos procedimientos y políticas, así como la identificación de brechas que requieran actualizar las normas establecidas para la gestión de riesgos.

4.2.1. Política de gestión de riesgos

Se deberá definir la política para la gestión de riesgos, la cual debe establecer los lineamientos a seguir para administrar los riesgos tecnológicos por las diferentes áreas del negocio, y establecer los responsables de los procesos críticos así como los lineamientos para gestionar los riesgos, evaluar los riesgos y responder a los riesgos. La política deberá ser clara y entendible por cualquier colaborador y deberá ser una guía para los gestores de riesgos que les permita identificar las acciones a seguir para gestionar los riesgos tecnológicos.

El contenido de la política de gestión de riesgos tecnológicos, deberá comprender:

- Objetivos: comprendido por un objetivo general y objetivos específicos. Donde el objetivo general deberá enfocarse en concientizar a los dueños de los procesos y responsables de TI de la existencia de riesgos, su necesidad de mitigarlos y proveer un modelo para gestionar los riesgos de forma oportuna que permita mantener bajo control los riesgos tecnológicos. En el caso de los objetivos específicos, deberán orientarse a los objetivos de la empresa por los cuales se implementa la gestión de riesgos tecnológicos.

- Alcance: acá deberá delimitarse la aplicación de la política especificando a qué nivel será aplicable y las áreas que estarán sujetas a la misma.

- Estructura organizacional: deberá definirse por medio de un organigrama como se conformara el equipo responsable de la gestión de riesgos estableciendo jerarquías y líneas de comunicación. Asimismo, deberá incluirse los manuales de puesto de los diferentes puestos que participen en la gestión de riesgos para identificar el perfil técnico, académico y capacidades necesarias por parte del personal a cargo del proceso.

- Marco jurídico: deberá identificarse las leyes, normas, políticas, regulaciones o normativas a las cuales se encuentre sujeta la organización y que tengan relación, dependencia o impacto en la gestión de riesgos tecnológicos; estas pueden ser internas como externas. Como por ejemplo, lineamientos de seguridad, políticas de accesos, políticas de uso de recursos informáticos, política de gestión de riesgos del negocio, entre otras.

- Funciones y responsabilidades: deberán definirse las funciones y responsabilidades de cada uno de los roles a cargo de la gestión de riesgos especificando las actividades a realizar, su periodicidad y el resultado esperado de cada puesto. Por ejemplo, responsable de aplicación de acciones correctivas, evaluación de riesgos, respuesta al riesgo, definición de controles, notificación de incidencias, entre otros.

- Descripción del marco metodológico: el cual deberá identificar las normativas adoptadas para la gestión de riesgos en nuestro caso se propone la incorporación del Framework Risk IT con una descripción de la misma; asimismo, deberá incluir el modelo de gestión de riesgos a utilizar que corresponde a las etapas que comprenden el ciclo repetitivo para la gestión de riesgos.

- Documentos relacionados: apartado en el cual deberán identificarse los procedimientos, estándares y normativas asociadas como referencia para consulta del lector de la política.

- Sanciones y casos no contemplados: deberá definirse como se accionara ante el incumplimiento de los lineamientos de la política y como se manejaran las excepciones o casos no contemplados. Las sanciones deberán estar sujetas a la política de recursos humanos.

4.2.2. Procedimientos para la gestión de riesgos

Corresponde a la definición de las actividades a seguir por parte de los diferentes responsables para gestionar los riesgos, estos podrán presentarse como diagramas de flujo o procesos descriptivos que establezcan la interacción entre los diferentes roles del negocio responsable de la gestión de riesgos, las actividades a realizar, las entradas y salidas de cada una de las actividades y los resultados finales. Los procedimientos que se deberán definir como mínimo, deberán incluir:

- Procedimiento para identificación y evaluación de riesgos
- Procedimiento para respuesta a riesgos
- Procedimiento para comunicación de riesgos
- Procedimiento para seguimiento, monitoreo y control de riesgos
- Procedimiento para documentar, modificar o actualizar la documentación para la gestión de riesgos

4.2.3. Normas para la gestión de riesgos

Acá deberán definirse lineamientos bajo los cuales debe accionar un colaborador para gestionar los riesgos no incluidos dentro de las políticas o procedimientos para la gestión de riesgos; por ejemplo métodos cualitativos o cuantitativos utilizados para evaluación de riesgos y normativas, mejores prácticas o estándares a seguir para la gestión de riesgos tecnológicos.

4.3. Fomentar la gestión de riesgos

Definido el nivel de madurez deseado y alineado a los objetivos estratégicos del negocio, con una claridad de las capacidades de TI que tiene la empresa y con una claridad de los responsables de la gestión de riesgos, se debe apoyar por los altos mandos la gestión de riesgos tecnológicos para que toda la empresa este alineada y cumpla con las acciones que se definan para la gestión de riesgos.

Para esto, desde los niveles más altos de la organización debe impulsarse el cambio cultural para la gestión de riesgos estableciendo directrices para que las diferentes áreas del negocio cumplan con las actividades y procesos definidos para la gestión de riesgos; de esta forma, la alta gerencia deberá apoyar y promover:

- La implementación de mecanismos y lineamientos de comunicación que permitan dar a conocer riesgos identificados, retroalimenten de la efectividad de respuesta a riesgos e informen del cumplimiento de actividades para minimizar o aprovechar oportunidades identificadas de riesgos conocidos.

- Implementación y publicación de políticas, procedimientos, normas o lineamientos para la gestión de riesgos los cuales permitan un adecuado control, seguimiento y monitoreo de los riesgos tecnológicos.

- Comunicación responsabilidades y compromisos a nivel de los diferentes roles responsables de la gestión de riesgos estableciendo funciones de supervisión, seguimiento y rendición de cuentas.

- Comunicación de metodologías, estándares o mejores prácticas a utilizar para la gestión de riesgos y herramientas que permitan eficientizar los resultados de la empresa por medio de la gestión de riesgos.

- Proveer recursos para automatizar tareas te control de riesgos dependiendo del nivel de madurez deseado, como por ejemplo la implementación de tecnología o software especifico para monitoreo y control de indicadores de riesgos tecnológicos.

4.4. Implementación del modelo de gestión de riesgos

El objetivo principal de la gestión de riesgos es contar con un proceso que permita identificar, evaluar y controlar eventos no deseados que impacten en recursos o servicios tecnológicos los cuales puedan afectar las operaciones de la organización generando efectos negativos. Para minimizar el riesgo al cual la empresa se encuentra expuesta es necesario aplicar las directrices de gestión de riesgos definidas por el Framework Risk IT para lo cual se deberán cumplir las actividades como parte del proceso de gestión de riesgos que se listan a continuación.

4.4.1. Definición del alcance de la gestión de riesgos

Para iniciar a gestionar los riesgos, es indispensable que determinen los límites de la evaluación de riesgos, los recursos con que se cuenta para la gestión y se identifique la información existente para la evaluación de riesgos. Para definir el alcance del análisis de riesgos, deberán tomarse en consideración los siguientes aspectos:

- Objetivos estratégicos del negocio: estos deberán estar alineados a los objetivos del área de TI según lo definido en la sección 4.1.1.

- Políticas internas de la organización: las cuales dictan los lineamientos internos que deben cumplir los colaboradores para desempeñar sus funciones de acuerdo a las operaciones que tengan asignadas según sus manuales de puesto.

- Procesos del negocio: como requisito principal, deberán haberse identificado los procesos principales del negocio de tal forma que el alcance contemplen el impacto y dependencia que tienen sobre los recursos y servicios tecnológicos según lo definido en la sección 4.1.4.

- Funciones y estructura organizacional: esta información es indispensable para establecer canales de comunicación, dueños de procesos y responsables de la gestión de riesgos por área.

- Requerimientos legales, contractuales y normativos: estos deberán estar contemplados en el marco jurídico de la política de gestión de riesgos definida de acuerdo a lo referido en la sección 4.2.1.

- Política de seguridad y de uso de recursos informáticos: estas son políticas internas que deberán estar identificadas en la política de gestión de riesgos informáticos según lo definido en la sección 4.2.1.

- Enfoque para la valoración del riesgo: enfoque ejecutivo definido por directores y gerentes a cargo del gobierno de la organización donde se definen los objetivos estratégicos de la gestión de riesgos tecnológicos como parte de los resultados esperados de la gestión empresarial. Incluye la definición umbrales de tolerancia al riesgo y la definición de la integración de riesgos tecnológicos con riesgos empresariales.

- Activos de información críticos: esta información debe generarse del análisis de capacidades de TI en donde deberá permitirse proporcionar el inventario de servicios y activos que posee la organización.

- Recursos disponibles (financieros, humanos): esta información permitirá determinar la capacidad que tiene la organización para asignar recursos a la gestión de riesgos tecnológicos.

4.4.2. Definición de criterios de evaluación, impacto y aceptación de riesgos

Para iniciar la Evaluación de riesgos, deberán definirse los criterios bajo los cuales deberá realizarse el análisis los cuales consisten en aspectos relevantes a considerar para establecer los niveles de tolerancia, apetito al riesgo e impacto en el negocio. Para definir estos criterios, se deberán tomar en consideración los aspectos que se definen a continuación.

4.4.2.1. Criterios para la evaluación de riesgos

Para evaluar el riesgo tecnológico al cual se encuentra expuesta la PYME, deberán considerarse los siguientes criterios:

- Nivel de criticidad del activo involucrado
- Requerimientos legales, regulatorios y contractuales
- Importancia en la operación y en el negocio de la disponibilidad, confidencialidad e Integridad
- Expectativas y percepción de interesados
- Consecuencias negativas sobre la imagen y reputación de la empresa

4.4.2.2. Criterios para determinar el impacto

Para determinar el impacto que representa al negocio cada uno de los riesgos identificados, deberán considerarse los siguientes criterios:

- Niveles de clasificación de los activos impactados. Se refiere a la magnitud del impacto si un riesgo llegara a materializarse
- Brechas en seguridad de la información (impacto que tendría a nivel de disponibilidad, confidencialidad e Integridad de la información)
- Problemas en operaciones
- Pérdidas financieras o del valor del negocio
- Retrasos o incumplimientos de planes de trabajo o fechas de entrega
- Brechas identificadas en relación a incumplimiento de requerimientos legales, contractuales o regulatorios

4.4.2.3. Criterios para la aceptación de riesgos

Considerando que los recursos son limitados y la gestión de riesgos genera un costo para la organización, deberán tomarse en consideración los siguientes criterios para el tratamiento y aceptación de riesgos:

- Criterios del negocio. Deben ser definidos por los dueños de los procesos del negocio y dependerá del apetito y tolerancia al riesgo definidos
- Aspectos legales, regulatorios y contractuales
- Aspectos propios de la operación
- Características, capacidades y disponibilidad de tecnología
- Recursos económicos o financieros
- Aspectos sociales

4.4.3. Identificación y documentación de riesgos

Esta etapa busca obtener una claridad y mejorar el conocimiento sobre el entorno de tecnología de la organización para lo cual se debe realizar un levantado de riesgos; proceso mediante el cual se deben identificar los activos a evaluar y determinar sus amenazas y vulnerabilidades. La recolección de esta información se realiza por medio de entrevistas, lluvias de ideas, encuestas, observaciones, análisis de eventos históricos en el contexto organizacional, revisión de documentos de la organización, informes de auditoría o análisis de riesgos anteriores.

El tener identificados los activos, amenazas y vulnerabilidades nos permitirá generar el portafolio de riesgos tecnológicos los cuales serán considerados como el potencial de que dada una amenaza, explote una

vulnerabilidad en un activo o grupo de activos que generan perdidas o daños a los activos, de donde podremos obtener la relación:

$$Riesgo = Activo * Amenaza * Vulnerabilidad$$

4.4.3.1. Identificación de activos

Para elaborar el inventario de activos tecnológicos o recurso de tecnología de información necesario para que la organización funcione adecuadamente en el cumplimiento de sus operaciones, es recomendable cumplir con los siguientes lineamientos para que estos sean de utilidad en el análisis de riesgos:

- Incluir todos los activos dentro del inventario categorizándolos por tipo de activo, como: equipos (hardware), servicios (que se prestan o se necesitan para gestionar información), intangibles, aplicaciones (software), documentos, servidores, bases de datos, interfaces y redes de comunicación.

- Para cada activo, identificar el propietario o responsable del activo tecnológico así como las personas que operan dichos activos.

- Establecer los derechos de acceso para cada uno de los activos tecnológicos.

- Documentar información general como por ejemplo, ubicación del activo, fecha de compra. Posteriormente en la evaluación del riesgo deberá complementarse la información adicionando el tipo de amenaza, riesgos,

impacto y la influencia del factor tiempo lo cual dependerá de los escenarios de riesgo identificados.

4.4.3.2. Identificación de amenazas

Identificados los activos, para cada uno deberán identificarse las amenazas a las cuales se encuentran expuestos tomando en consideración que las amenazas entre los activos difieren de tal forma que no todas las amenaza afectan a todos los activos sin embargo debe identificarse lo que puede ocurrir en cada activo por cada amenaza.

Como entregable deberá generarse un catálogo de amenazas tecnológicas que debe identificar la fuente u origen de la amenaza pudiendo ser:

- Natural: inundaciones, terremotos, tornados, huracanes, derrumbes o deslaves, tormentas eléctricas, sismos, polvo, entre otras.

- Humanas: acciones realizadas por personas ya sea de forma involuntaria (por ejemplo: ingreso o registro de datos incorrectos, desconocimiento de procedimientos), premeditada (ataques de seguridad, acceso no autorizado a información confidencial, infección de virus, hacking) o por negligencia (incumplimiento de procedimientos, incumplimiento o mal manejo de estándares).

- Ambientales: contaminación, apagones, sobrecarga de capacidades, incendio, entre otros.

En el caso de fuentes humanas, debe tomarse en consideración que son potencialmente peligrosas debido a la motivación y los recursos que pueden tener para realizar algún tipo de ataque que ocasiones la materialización de un riesgo identificado; de esta forma, podemos catalogarlos como:

- Cyber criminales o criminales computacionales
- Espionaje industrial
- Personal interno (perteneciente a la organización)

4.4.3.3. Identificación de vulnerabilidades

Como base para identificar las vulnerabilidades se deberán tomar en consideración las amenazas identificadas ya que una vulnerabilidad no es más que la capacidad, condiciones y características de los activos que los hace susceptible a una amenaza. Una vulnerabilidad se considera como un defecto o debilidad en procedimientos de seguridad, deficiencia en el diseño o implementación de controles que pudieran ser superados sobrepasando los niveles de seguridad implementados.

Las vulnerabilidades deberán quedar documentadas y para identificarlas se recomienda tomar en consideración los siguientes tips:

- Definir una lista de requerimientos de seguridad
- Realizar pruebas de seguridad de los sistemas
- Cuestionar que sucedería si un evento ocurriera

4.4.4. Evaluación y medición de riesgos

La evaluación de riesgos se basa en la medición del impacto y la frecuencia que se determina en función a escenarios o criterios de categorización que permiten clasificarlo según su periodicidad de ocurrencia y la intensidad o impacto, lo cual se puede identificar utilizando el mapa de riesgos definido en la sección 1.3.2. Esta evaluación es subjetiva dado que se realiza por el responsable del proceso en base a su experiencia, sin embargo permite detectar fortalezas y debilidades del ambiente tecnológico y, los riesgos potenciales a los cuales se encuentran expuestos.

Como parte de la evaluación de riesgos, deberá realizarse una descripción de los riesgos, determinar por cada riesgo la probabilidad de ocurrencia y el impacto en el negocio o área de negocio según sea el caso, identificar y evaluar los controles existentes, calificar el nivel de riesgo inherente, determinar los puntos de mejoras y establecer indicadores que permitan medir la efectividad en la gestión de riesgos.

Las herramientas que deberán utilizarse para identificar los riesgos comprenden reportes de auditoría de sistemas, autoevaluaciones, mejores prácticas (COBIT 5.0, ISO, entre otras), Indicadores de riesgos, acontecimientos históricos de la pérdida o conocimiento cercano a la perdida y los mapas de riesgos. Los escenarios de riesgos a considerar dentro de la evaluación, según The Risk Practitioner Guide de ISACA, deberán incluir los que se muestran en la matriz de la tabla VIII.

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

Ámbito del escenario de riesgo	Escenario de riesgo
Infraestructura física de TI	Obsolescencia
	Daño o destrucción
	Robo
	Arquitectura inadecuada
	Instalación y cambios
Relacionados con personal de TI	Ausencia de 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 del portafolio de proyectos
Gestión de seguridad	Ataque lógico a la seguridad
	Traspasar la seguridad
	Alteración de integridad de la información
	Exposición de la información
Aplicaciones	Decisiones incorrectas de inversión en aplicaciones
	Caducidad de las aplicaciones del negocio
	Implementación inadecuada de aplicaciones
	Inestabilidad de aplicaciones
	Falta de capacidad de las aplicaciones
	Caducidad de aplicaciones de infraestructura
	Aplicaciones intrusas

Continuación de la tabla VIII.

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	Cumplimiento legal en Guatemala
Otros escenarios	Rendición de cuentas de TI
	Integración de TI y procesos del negocio
	Errores operativos de TI
	Procesos operativos de TI

Fuente: The Risk IT Practitioner Guide.

4.4.4.1. Determinación de la frecuencia

Esta actividad consiste en determinar la probabilidad de ocurrencia de un riesgo o vulnerabilidad potencial y para definirla deberá considerarse la naturaleza de la vulnerabilidad, la motivación o la capacidad de la fuente de amenaza. La clasificación de la frecuencia deberá darse de acuerdo a la siguiente tabla.

Tabla IX. **Clasificación de probabilidad de ocurrencia de un riesgo**

Clasificación	Frecuencia	Descripción
5	Esperado	Cuando los eventos ya se han presentado o pueden presentarse a menudo, son comunes y constantes

Continuación de la tabla IX.

4	Muy probable	Cuando los eventos se han presentado o pueden presentarse de manera común
3	Probable	Cuando la incidencia de riesgo se ha presentado o puede presentarse de forma frecuente durante un periodo de tiempo determinado
2	Poco probable	Cuando los riesgos identificados se han presentado o pueden presentarse de forma ocasional
1	Remoto	Cuando la incidencia de riesgo es inusual o que nunca se ha presentado

Fuente: Adaptación clasificación de frecuencia, *Manual Normativo de Riesgo Tecnológico*.

4.4.4.2. Determinación del impacto

Esta actividad consiste en determinar el daño que se genera sobre el activo al momento de materializarse una amenaza; para determinar el impacto debe tomarse en consideración los factores relacionados al activo evaluado como por ejemplo la perdida de confidencialidad, integridad o disponibilidad.

El impacto deberá clasificarse de acuerdo a los criterios definidos en la tabla X.

Tabla X. **Clasificación de impacto por materialización de amenazas**

Clasificación	Impacto	Descripción
5	Crítico	Riesgo severo que al materializarse genera pérdidas altamente costosas para la organización y pueden impactar en el patrimonio o generar pérdida de ingresos
4	Alto	riesgo severo que al materializarse puede interrumpir las operaciones de la organización de forma parcial
3	Moderado	Pérdida considerable derivado de una contingencia ante el riesgo que puede generar inconvenientes significativos en la organización
2	Bajo	Perdida menor derivada de riesgos que pueden provocar inconvenientes en la organización
1	Menor	Perdida mínima derivada de riesgos que no impactan en la productividad de la organización o que generan inconvenientes menores y manejables

Fuente: Adaptación clasificación de Impacto, *Manual Normativo de Riesgo Tecnológico*.

4.4.4.3. Ponderación de factores de riesgo

Luego de concluir la definición de frecuencia e impacto para los riesgos inherentes identificados, se deberán graficar los riesgos en el mapa de riesgos tecnológicos definidos en la sección 1.3.2. Esto nos permitirá contar con un listado de riesgos absolutos bajo un enfoque cualitativo que refleja el nivel de exposición que se tiene por cada uno de los riesgos. La tabla XI muestra los

niveles de exposición que puede tomar un riesgo los cuales son de utilidad para identificar los riesgos críticos para poder priorizar la evaluación y atención de los mismos y, definir los controles necesarios que permitan mitigar la exposición dentro de los niveles de tolerancia que defina la organización.

Tabla XI. **Clasificación nivel de exposición de riesgos**

Clasificación	Exposición	Descripción
5	Extremo	Riesgo con gran probabilidad de ocurrencia e impacto critico al llegar a materializarse
4	Alto	Riesgo con alta probabilidad de ocurrencia y fuerte impacto al llegar a materializarse
3	Medio	Riesgo con probabilidad media de ocurrencia e impacto significativo al llegar a materializarse
2	Moderado	Riesgo con probabilidad de ocurrencia e impacto considerable al llegar a materializarse
1	Bajo	Riesgo con mínima probabilidad de ocurrencia e impacto menor al llegar a materializarse

Fuente: Adaptación clasificación de Impacto, *Manual Normativo de Riesgo Tecnológico*.

4.4.4.4. Análisis de controles

Identificados los riesgos tecnológicos a los cuales se encuentra expuesta la organización, se deben establecer los mecanismos para prevenir o reducir el impacto que pueden ocasionar eventos no deseados para lo cual deben implementarse controles que pueden ser técnicos (hardware o software) o no técnicos (políticas de seguridad, procedimientos administrativos, procedimientos operacionales y seguridad física).

Los controles a definir deberán ser suficientes, comprensibles, eficaces y oportunos; para definirlos deberá tomarse en consideración la naturaleza del riesgo, frecuencia, impacto e implicaciones para garantizar la continuidad de las operaciones.

Los controles definidos deberán ser documentados justificando su aplicación e identificando el o los riesgos a los cuales serán aplicados, asimismo deberá definirse su naturaleza, pudiendo ser:

- Preventivo: los cuales buscaran disminuir la probabilidad de ocurrencia y formaran parte de la primera línea de defensa de la organización reduciendo el accionar de los agentes generadores de riesgo.

- Defectivo: los cuales buscan descubrir un evento, irregularidad o resultado no provisto en el momento en que se presentan, alertando de la presencia del riesgo y permitiendo tomar medidas inmediatas en respuesta al riesgo.

- Correctivo: los cuales permiten restablecer las operaciones después de la detección del evento no deseado y modificar las acciones que propiciaron su ocurrencia.

- Manual: son los que se ejecutan por parte de personas especificas de acuerdo a sus funciones y pueden ser planificados o no planificados.

- Automatizados: son los ejecutados por un sistema de información.

El anexo D, muestra un inventario de controles sugeridos para cada uno de los escenarios de riesgos listados en la tabla VIII, los cuales han sido

propuestos en el Framework Risk IT de ISACA en el documento The Risk IT Practitioner Guide.

4.4.4.5. Determinar el riesgo residual y niveles de tolerancia

El riesgo residual deberá calcularse después de la implementación de controles ya que este tiene un efecto sobre la ponderación de la frecuencia e impacto de cada uno de los riesgos, se calcula para cada uno de los riesgos identificados utilizando la siguiente fórmula:

$$Riesgo\ residual = \frac{(frecuencia * impacto)}{control}$$

El resultado del riesgo residual debe ser clasificado para determinar los niveles de tolerancia de los riesgos para lo cual deberán utilizarse la siguiente clasificación:

- Aceptable: cuando se obtiene un resultado por debajo de 1
- Tolerable: cuando el resultado se encuentra entre 1 y 3
- Por arriba de lo aceptable: cuando el resultado es superior a 3

De acuerdo a los niveles de tolerancia derivados del riesgo residual, los riesgos deberán clasificarse definiendo cuáles son los que requieren alguna acción, ya sea aplicando medidas correctivas, fortalecimiento de controles o monitoreo. Para documentarlos y clasificarlos se podrán utilizar los criterios definidos en la tabla XII, lo cual deberá considerarse en la toma de decisiones y para priorizar la mejora de los controles existentes o implementación de nuevos controles.

Tabla XII. **Niveles de tolerancia de riesgos**

Clasificación	Nivel de Tolerancia	Medida Correctiva
3	Por arriba de la tolerancia	Establecer un plan de acción correctivo cuanto antes
2	Tolerable	Establecer un plan de acción correctivo en un periodo de tiempo razonable para la organización
1	Aceptable	Requieren monitoreo y considerar oportunidades de mejora en la implementación de controles

Fuente: elaboración propia.

4.4.5. Priorización y definición de respuesta al riesgo

Considerando que los recursos con que se cuentan dentro de la organización son limitados, está etapa pretende que se definan cuales son aquellos riesgos que afectan a la organización para definir una acción a realizar en un tiempo determinado sobre las exposiciones relevantes. Para priorizar los riesgos mediante la jerarquización se debe tomar en consideración el resultado del riesgo residual y su nivel de tolerancia.

Definida la jerarquía de atención de riesgos, se debe tomar la decisión de la respuesta que se dará a cada riesgo tomando un enfoque costo/beneficio; el comité de gestión de riesgos deberá decidir el tratamiento que se dará a cada riesgo de acuerdo a los tipos de respuesta posibles definidos en la sección

1.4.5, los cuales pueden ser: evitar el riesgo, mitigar o reducir el riesgo, transferir o compartir el riesgo, o aceptar el riesgo.

4.4.6. Plan de tratamiento del riesgo

Hasta el momento se tienen identificados, priorizados y definidas las respuestas que se darán a los riesgos identificados; para poder mitigarlos deberá establecerse un plan de tratamiento de riesgos el cual debe involucrar no solo al personal asignado para gestión de riesgos sino a los miembros de las áreas que se ven involucradas o afectadas por estos riesgos.

Para que el plan de tratamiento de riesgos sea efectivo, se deberán comunicar los riesgos así como su exposición y recomendar los controles a implementar para mitigar los riesgos basándose en los criterios de aceptación de riesgo previamente definidos de tal forma que las medidas que se establezcan permitan proteger los intereses de la organización y las áreas involucradas.

El plan de trabajo a presentar deberá definir las acciones concretas a realizar, responsables por actividad y los periodos de tiempo en los cuales serán implementadas cada una de las tareas definidas. Este plan deberá ser aprobado por el comité o responsable de riesgos designado y conciliado con las áreas involucradas para que asignen el recurso necesario.

4.4.7. Monitoreo

Para garantizar la eficacia de las acciones realizadas para mitigar los riesgos tecnológicos, es necesario contar con un mecanismo que permita

establecer la eficacia de las acciones que se realizan para dar respuesta a los riesgos según los lineamientos definidos por el comité de gestión de riesgos.

En esta etapa deberán definirse los indicadores que deben ser utilizados para medir la efectividad de las actividades de los controles. Los indicadores a definir deberán ser fáciles de medir, de fácil acceso y con una fuerte correlación con los riesgos.

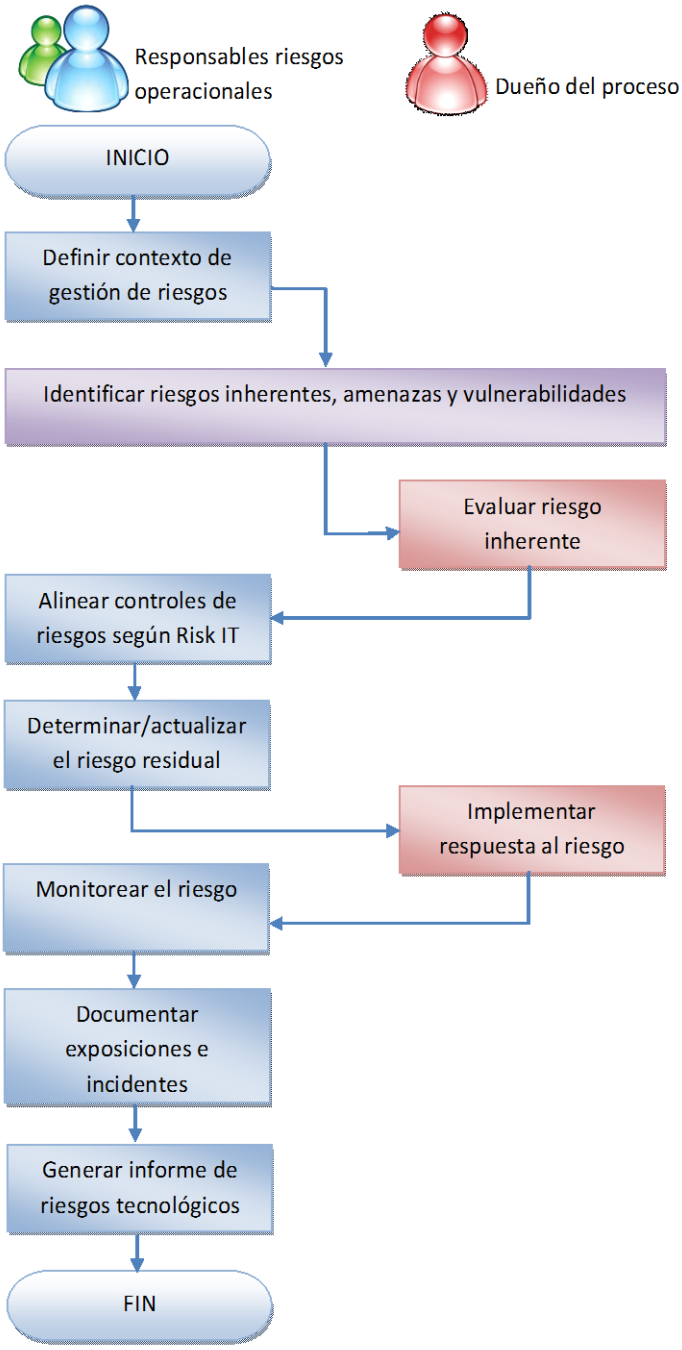
Para la definición de indicadores deberán tomarse en consideración los aspectos definidos en la sección 1.4.5, considerando que cada KRI se encuentra relacionado con al apetito al riesgo y la tolerancia para que los niveles de activación se puedan definir permitiendo a los Stakeholders tomar las medidas adecuadas en el momento oportuno.

Asimismo, deberán definirse indicadores de desempeño, de procesos y de metas de TI.

4.5. Definición de procedimiento de gestión de riesgos

Considerando que la gestión de riesgos es un proceso repetible que debe garantizar la mejora continua en los controles asociados a los riesgos y en los indicadores de desempeño, de tal forma que estos se mantengan actualizados y puedan cumplir con sus funciones en un entorno tecnológico cambiante, se propone el modelo de la figura 14 para la gestión de riesgos, el cual deberá ser adaptado a las necesidades y capacidades de la organización.

Figura 14. **Procedimiento gestión de riesgos tecnológicos**



Fuente: elaboración propia.

4.6. Gestión de comunicación

Uno de los principales factores por las que fallan los procesos es por no establecer una buena comunicación sobre los mismos, sus objetivos y responsabilidades de cada uno de los miembros de la organización. Por lo cual es indispensable que al contar con el modelo definido para la gestión de riesgos, este se comunique y difunda a todas las áreas para que estén enteradas.

La comunicación deberá ser organizada, estructurada y dirigida a las personas correctas, en el momento oportuno y aprovechando los recursos o medios con los cuales cuenta la organización. Para realizar una correcta comunicación se sugiere:

- Establecer un plan de comunicación que ponga a disposición de las personas correctas la información necesaria en el momento oportuno.

- Especificar a detalle las formas de comunicación que se utilizaran (comunicación directa, teléfono, correo electrónico, carpetas de red compartidas, documentación impresa, presentaciones, medios electrónicos, herramientas que centralicen información, por la nube, etcétera), la periodicidad con que se tendrá disponible la información y los responsables de realizar la comunicación.

- Definir los roles y responsabilidades de los involucrados en el proceso de tal forma que se tenga claridad de quienes crean, autorizan, modifican o leerán la información.

4.7. Seguimiento y supervisión de la gestión de riesgos

Esta etapa consiste en realizar procesos cíclicos para determinar que se cumplen con los procesos definidos, que los controles realizan las funciones para lo cual fueron creados y que los responsables dentro del proceso de gestión de riesgos tecnológicos realizan las operaciones designadas alineados al modelo de gestión de riesgos, normas internas y externas, y el marco de referencia adoptado.

Acá debe verificarse que cada activo de tecnología que es evaluado, cuente con los controles adecuados para mitigar los riesgos, se deben evaluar los resultados de las métricas establecidas y monitorear que los riesgos se mantienen dentro de los niveles de tolerancia definidos.

Las acciones a realizar para por personal interno de TI, auditoría interna o entidades externas deberán incluir:

- Evaluación que se haya alcanzado el nivel de madurez definido como parte del plan de gestión de riesgos.

- Validar que la inversión de tiempo y recursos para proteger los activos se encuentran definidos de acuerdo a la importancia que representa el activo.

- Informar acerca de los resultados obtenidos de la evaluación a nivel directivo, responsable de TI y responsables de la gestión de riesgos.

- Generar información para el proceso de mejora continua que debe definirse en base a recomendaciones de mejoras de controles existentes o diseño de nuevos controles.

Como parte del seguimiento, deberá determinarse la eficacia de cada control lo cual permitirá conocer el nivel de madurez alcanzado pudiendo utilizar la siguiente tabla de ponderaciones.

Tabla XIII. **Ponderación eficacia de controles de riesgos**

Ponderación	Descripción
5	Los procedimientos y medidas de control se encuentran automatizados, formalizados y siempre son utilizados, aplicados, medidos y monitoreados
4	Los procedimientos y medidas de control se encuentran formalizados y siempre son utilizados, aplicados, medidos y monitoreados
3	Los procedimientos y medidas de control se encuentran formalizados, siempre son utilizados y aplicados
2	Los procedimientos y medidas de control no están formalizados y no siempre son utilizados o aplicados
1	Se tiene consciencia sobre la necesidad de contar con procedimientos o medidas de control pero no se cuenta con ellos
0	No se cuenta con políticas o procedimientos para la gestión del riesgo

Fuente: Adaptación ponderación de riesgos, *Manual Normativo de Riesgo Tecnológico*.

La ponderación de la tabla XIII permite determinar el riesgo residual con el cual se podrá saber si se ha obtenido una mejoría en la gestión de riesgos.

4.8. Mejora continua

Por último, se deberá garantizar que el modelo de gestión de riesgos se mantendrá actualizado y en continuo perfeccionamiento de tal forma que los resultados de las evaluaciones de riesgos permitan determinar la situación actual y en base a las recomendaciones brindadas se inicien procesos de cambio los cuales serán la base para iniciar un proceso de mejora continua.

4.9. Actividades para mitigar el riesgo tecnológico

La tabla XIV lista las actividades que deberán realizarse para poner en marcha el plan de mitigación del riesgo tecnológico en la PYME evaluada; estas deberán ejecutarse de forma secuencial quedando a cargo de los responsables establecidos para cada uno de los diferentes roles que se involucran en él plan; asimismo, se incluye el tiempo sugerido en el cual debe realizarse cada una de las actividades.

Tabla XIV. **Actividades sugeridas para mitigar el riesgo**

ID	Actividad	Responsables*	Duración Sugerida
1	Alinear los objetivos del negocio a los objetivos de TI	DE, RT	2 días
2	Evaluar la capacidad de TI	RT	4 días
3	Definir el nivel de madurez deseado	DE, RT	2 días
4	Definir roles y responsabilidades para la gestión de riesgos	DE, RT	2 días
5	Definir estructura administrativa para la gestión de riesgos	DE, RT	2 días
6	Definir comité de riesgos	DE, RT	1 día

Continuación de la tabla XIV.

7	Definir responsable gestión de riesgos (OST)	CR	1 día
8	Identificar principales líneas de negocio y procesos prioritarios	CR, OST, RT	20 días
9	Definición de políticas, procedimientos y normas para la gestión de riesgos	CR, OST, RT	8 días
10	Dar a conocer y fomentar proceso de gestión de riesgos	DE, CR	1 día
11	Definición del alcance de la gestión de riesgos	CR, OST, RT	2 días
12	Definición de criterios de evaluación, impacto y aceptación de riesgos	CR, OST, RT	2 días
13	Elaboración de inventarios de activos de TI	RT, OST	3 días
14	Identificación de amenazas	OST	4 días
15	Identificación de vulnerabilidades	OST	5 días
16	Listado de riesgos tecnológicos	OST	5 días
17	Determinar frecuencia de riesgos	OST	2 días
18	Determinar el impacto de riesgos	OST	3 días
19	Ponderación de factores de riesgos	OST	3 días
20	Análisis y definición de controles	OST, RT	5 días
21	Determinación de riesgo residual	OST	3 días
22	Priorización y definición de respuesta a riesgos	OST, CR	4 días
23	Definición de plan de tratamiento de riesgos	OST, RS	10 días
24	Definición de indicadores de desempeño	OST, CR, RS	5 días
25	Definición de proceso de gestión de riesgos	CR, OST	2 días
26	Análisis y diseño herramienta para control de riesgos	OST, RT	5 días
27	Desarrollo de herramienta para control de riesgos	RT	15 días
28	Implementación controles de riesgos	RT	8 días
29	Evaluación de riesgos	OST, RS	45 días
30	Informe de evaluación de riesgos	OST	5 días
31	Revisión de Informe de evaluación de riesgos	CR	5 días
32	Toma de decisiones sobre gestión de riesgos	CR	2 días
33	Asignación de prioridades de gestión de riesgos	CR	2 días

* DE - dirección ejecutiva, RT - responsable de TI, CR - comité de riesgos, OST - oficial de seguridad tecnológica, RP - responsables de procesos

Fuente: elaboración propia.

CONCLUSIONES

1. La gestión de riesgos de TI en una organización es fundamental para evitar pérdidas que impacten las operaciones del negocio, así como, una herramienta valiosa para generar valor y apoyar a las operaciones del negocio por medio de la aplicación de acciones definidas en pro de mitigar los riesgos a los cuales se encuentra expuesta una organización.

2. La gestión de riesgos de TI deberá estar alineada a los objetivos estratégicos del negocio, a la gestión de riesgos del negocio y en general con ERM, para eficientizar la gestión del gobierno organizacional.

3. Toda empresa dependiente de TI para la gestión de sus operaciones, está expuesta a diversos factores de riesgo que va en relación al nivel de dependencia que tienen en TI; su mitigación está dada en base a las acciones, respuestas, planes y proyectos que implemente para incrementar el nivel de madurez que poseen para la gestión de riesgos. Mientras más dependientes de TI mayor será la exposición al riesgo.

4. Las PYME al conocer el riesgo al cual se encuentran expuestas por la dependencia que tienen sus operaciones de las TI, gestionan el riesgo con actividades definidas de acuerdo a las experiencias, con lo cual se ubican en un nivel de madurez “inicial” para la gestión de riesgos tecnológicos. Por la forma en que se gestiona el riesgo, ponen en riesgo las operaciones de la empresa, por lo cual es necesario contar con un marco de referencia que les permita minimizar la exposición al riesgo que presentan para dar una mejor respuesta a los riesgos.

5. El marco de referencia Risk IT es una herramienta útil para cualquier empresa que permite adaptarse de acuerdo a las necesidades, niveles de tolerancia y recursos que tiene la empresa; por lo cual se toma como base para plantear un plan de acción que brinda la oportunidad de mejorar el nivel de madurez de la gestión de riesgos para una PYME.

RECOMENDACIONES

1. Para minimizar la exposición a riesgos de TI, las PYME deben iniciar con evaluar su nivel de madurez, posterior a esto deben trabajar en políticas, procedimientos y planes de acción para medir la exposición al riesgo que presentan.

2. Al identificar los niveles de ejecución, se sugiere implementar la gestión de riesgos de TI evaluando los dominios de Risk IT para implementar los procesos que se adaptan a la empresa, lo indispensable es iniciar y dar continuidad al proceso de mejora continua como lo sugiere el Framework Risk IT.

3. Para lograr una gestión integral de los riesgos es necesario alinear la gestión de riesgos tecnológicos con la gestión de riesgos del negocio y a su vez, a la estrategia del negocio para que las tres se orienten en el mismo sentido.

4. Se debe establecer un procedimiento de comunicación de tal forma que la gestión de riesgos se expanda a través de toda la estructura de la organización definiendo responsabilidades, compromisos y sobre todo, que todos los colaboradores sean parte de los planes de respuesta para que puedan accionar ante la materialización de un riesgo.

5. Para maximizar los resultados de la gestión de riesgos y proveer nuevas oportunidades que maximicen el retorno de inversión en tecnología, es de vital importancia considerar la implementación de los marcos de

referencia COBIT y VAL IT para gestionar de una mejor forma los eventos internos y externos a la empresa, de tal forma que puedan plantearse nuevas soluciones que maximicen los resultados de la empresa.

BIBLIOGRAFÍA

1. AVIZIENIS, A.; LAPRIE, J.C.; RANDELL, B. *Fundamental Concepts of Dependability*, Research Report N01145, LAAS-CNRS. 2001. 20 p.

2. BISOGNO, María V. *Metodología para el aseguramiento de entornos informatizados – MAEI*. Argentina: Universidad de Buenos Aires, 2004. 234 p.

3. Committee of Sponsoring Organizations. *Enterprise Risk Management – Integrated Framework* [en línea]. USA. <http://www.coso.org/erm-integratedframework.htm> [Consulta: febrero de 2014].

4. Diario de Centro América. *La gestión del riesgo tecnológico* [en línea]. <http://www.dca.gob.gt/index.php/section-table-2/item/933-la-gesti%C3%B3n-del-riesgo-tecnol%C3%B3gico.html> [Consulta: abril de 2014].

5. ERB, Markus. *Gestión de riesgo en la seguridad informática* [en línea]. <http://protejete.wordpress.com/glosario/> [Consulta: mayo de 2014].

6. FERNÁNDEZ DE LARA, Carlos. *Seguridad de las empresas, comprometida por novatos:* Verizon [en línea]. b:Secure. <http://www.bsecure.com.mx/ultimosarticulos/seguridad-de-las-empresas-comprometida-por-novatos-verizon/> [Consulta: diciembre de 2013].

7. HIDALGO, N. A. *Una introducción a la gestión de riesgos tecnológicos* [en línea]. España: Universidad Politécnica de Madrid. <http://www.madrimasd.org/revista/revista23/tribuna/tribuna1.asp> [Consulta: enero de 2014].

8. INFONAVIT. *Manual normativo de riesgo tecnológico* [en línea]. Subdirección General de Planeación y Finanzas, Coordinación de Riesgos. <http://boletin.dseinfonavit.org.mx/035/documentos/ManualNormativodeRiesgoTecnologico.pdf> [Consulta: 8 de marzo de 2014].

9. Information System Audit and Control Association. COBIT 5.0, *Control Objectives for Information and Related Technology* [en línea]. <http://www.isaca.org/COBIT/Pages/default.aspx> [Consulta: febrero de 2014].

10. _____. *Marco de riesgos de TI*. ISBN 978-1-60420-111-6 [en línea]. <http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Spa_0610.pdf> [Consulta: 6 de marzo de 2014].

11. _____. *The Risk IT Framework*. ISBN 978-1-60420-111-6 [en línea]. <http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf> [Consulta: 5 de junio de 2014].

12. _____. *The Risk IT Practitioner Guide*. ISBN 978-1-60420-116-1 [en línea]. <http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Practitioner-Guide_res_Eng_0610.pdf> [Consulta: 5 de junio de 2014].

13. ISACA JOURNAL. *The Minimum IT Controls to Assess in a Financial Audit (Part I)* [en línea]. <http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/1001-the-minimum-IT.pdf> [Consulta: enero de 2014].

14. LÓPEZ, José; LUJAN, José. *Ciencia y política del riesgo*, Madrid: Alianza Editorial, 2000. 213 p.

15. RAMÍREZ, O.J. *Riesgos de origen tecnológico, apuntes conceptuales para una definición, caracterización y reconocimiento de las perspectivas de estudio del riesgo tecnológico* [en línea]. Manizales, Colombia. <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-24742009000200009> [Consulta: enero de 2014].

16. ROMERAL, Luís M.; TORRES G., Álvaro. *Gestión de los riesgos tecnológicos* [en línea]. RPM-AEMES Vol. 5 No. 1, ISSN: 1698-2029. Everis. <http://www.aemes.org/index.php/seminarios/seminarios-de-aemes/revista-de-procesos-y-metricas/ano-2008-volumen-5/volumen-5-g-numero-1-g-enero-2008/183-gestion-de-los-riesgos-tecnologicos> [Consulta: 8 de marzo de 2014].

17. SERRANO, Carlos. *Regulación internacional sobre auditoria informática, riesgos y seguridad en los sistemas de información.* España: Universidad de Zaragoza - *Una guía de seguridad informática* [en línea]. <http://ciberconta.unizar.es/LECCION/seguro/100.HTM> [Consulta: marzo de 2014].

18. Superintendencia de Bancos de Guatemala. *Reglamento para la administración integral de riesgos* [en línea]. Resolución Junta Monetaria JM-056-2011. <http://www.sib.gob.gt/c/document_library/get_file?folderId=455681&name=DLFE-9147.pdf> [Consulta: 25 de enero de 2014].

19. _____. *Reglamento para la administración del riesgo tecnológico* [en línea]. Resolución Junta Monetaria JM-102-2011. <http://www.sib.gob.gt/c/document_library/get_file?folderId=455681&name=DLFE-9901.pdf> [Consulta: 25 de enero de 2014].

20. Standards Australia. *Risk Management Guidelines Companion to AS NZS 4360 2004*. ISBN 0 7337 5960 2, Australia.

21. VEGA, Andrea. *Las 10 mejores prácticas en seguridad* [en línea]. <http://seguinfo.wordpress.com/2007/07/05/las-10-mejores-practicas-en-seguridad/> [Consulta: abril de 2014].

22. VERIZON. *Informe sobre investigación de brechas en los datos de 2012*. MC15244 ES 03/12 [en línea]. <http://www.verizonenterprise.com/resources/reports/rp_Informe_Sobre_Investigaciones_de_brechas_2012_es_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z055> [Consulta: 27 de enero de 2014].

23. _____. *Informe sobre investigación de brechas en los datos de 2013*. ES15581 (A4) ES 4/13 [en línea]. <http://www.verizonenterprise.com/resources/reports/es-informe-sobre-investigaciones-de-%20brechas-en-los-datos-de-2013_%20es_xg.pdf> [Consulta: 21 de junio de 2014].

24. _____. *Informe sobre investigaciones de brechas en los datos de 2014*. ES15921 ES 4/14 [en línea]. <http://www.verizonbusiness.com/resources/reports/rp_dbir-2014-executive-summary_es_xg.pdf> [Consulta: 21 de junio de 2014].

25. WESTERMAN, G.; HUNTER, R. *IT Risk: Turning Business Threats Into Competitive Advantage*. USA: Harvard Business School Press, 2007. 240 p.

APÉNDICE

Encuesta: evaluación nivel de madurez gestión de riesgos de TI / respuestas PYME

Encuesta de valoración para el proceso de gestión de riesgos		
A continuación se presenta una serie de preguntas para analizar qué actividades se realizan en su organización para gestionar el riesgo asociado a TI buscando determinar el nivel de abstracción que se tiene para minimizar los riesgos asociados a TI, aplicación de estándares y nivel de madurez basado en RISK IT.		
Nombre de Empresa a la que representa:	ALMACENES JAPON, S.A.	
Puesto que Desempeña	IMPLEMENTADOR DE SISTEMAS	
Cantidad de Usuarios a los que dan Servicio	100 - 500	
PRIMERA SECCIÓN: Análisis de generalidades y aplicación de estándares para la gestión del riesgo de TI.		
Instrucciones: Responda las siguientes preguntas de acuerdo el nivel de conocimiento que tiene dentro de su ambiente laboral		
1	¿Se administran riesgos que puedan afectar al negocio?	SI
2	¿Se administran riesgos específicos de TI con un responsable designado?	SI
3	¿En su organización existe un inventario, portafolio, perfil de riesgos o matriz de riesgos asociados a TI?	NO
4	¿Se aplica una metodología, estándar, mejores prácticas, marco de referencia o herramienta para la gestión del riesgo? En caso de contar con alguna, Especifique: _Propietaria_____ (P. Ej.: COBIT, ITIL, ISO, ERM, Risk IT, Propietaria)	SI
5	¿Se cuenta con normas, procedimientos o políticas que describen los lineamientos a seguir para gestionar los recursos y servicios relacionados a TI? (P. Ej.: solicitud de accesos, manejo de información, uso de correo electrónico, uso de internet, uso de equipo de computo, entre otros)	Si
6	¿Se cuenta con controles que permiten identificar o alertar la existencia de un riesgo relacionado con TI? (P. Ej.: interrupción de servicios, caídas de rendimiento, atraso en proyectos, accesos no autorizados, cercanía a umbrales de tolerancia en servicios, entre otros)	No Existen
7	¿Existe una matriz de responsabilidades RACI que permite identificar las principales actividades a realizar para gestionar el riesgo estableciendo responsables y tipo de responsabilidad?	NO
8	¿Sabe que acciones realizar en caso de identificarse la exposición, ocurrencia o materialización de un riesgo y como mantenerlo en los umbrales de tolerancia aceptados por la organización? (P. Ej.: Incumplimiento de cronogramas de trabajo por proveedor, interrupción de servicios como electricidad, perdida de información, fallas de aplicaciones y denegación de servicio)	Si, No estan Documentadas
9	¿Existen planes estratégicos que aprovechan la tecnología para obtener beneficios, maximizar el valor por medio de nuevos productos, servicios innovadores o nuevas oportunidades de negocio?	Si

Continuación de la encuesta.

SEGUNDA SECCIÓN: Medición de frecuencia con que se realizan actividades relacionadas a la gestión de riesgos dentro de su empresa.

Instrucciones: Marque con una "X" la respuesta (columna) más acorde a la frecuencia con la cuál se realiza la actividad descrita en la pregunta. La columna "Score" tomara de forma automática el valor entre 0 y 5, donde 0 significa que la organización no cumple con el requerimiento en lo absoluto y 10 que el requerimiento se cumple en su totalidad.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
GOBIERNO DE RIESGOS: Establecer y Mantener una visión común de riesgos							
RG1.1	**Evaluación de riesgos de TI en la empresa**						
10	¿Se realizan talleres para determinar el nivel de riesgo que la organización esta dispuesta a aceptar en el camino hacia la consecución de sus objetivos estratégicos?	x					0
11	¿La administración de TI ayuda a la empresa a comprender los riesgos de TI en el contexto de escenarios que afectan el negocio y sus objetivos estratégicos (P. Ej.: Ventas, Costos, Satisfacción del Cliente, Dinero)				x		3
12	¿Se realiza una análisis top-down, end-to-end de los servicios empresariales para determinar los principales puntos de soporte de TI?				x		3
13	¿Se realiza un análisis para identificar donde se genera valor, donde debe ser protegido y ser sostenido?		x				1
14	¿Se identifican eventos relacionados con las TI y las condiciones que pueden poner en riesgo el valor, afectan el desempeño de la empresa y la ejecución de actividades críticas del negocio dentro de parámetros aceptables o que de otro modo afectan los objetivos de la empresa (P. Ej.: negocios, regulatorios, jurídicos o legales, contratos, tecnológicos, socios comerciales, recursos humanos, otros aspectos operacionales)			x			2
15	¿Se realiza un mapa de riesgos impulsado por el negocio que categoriza y subcategoriza los riesgos derivados de los escenarios de riesgo de TI de alto nivel?				x		3
16	¿Se dividen los riesgos de TI por líneas de negocio, producto, servicio y procesos?					x	4
17	¿Se identifican posibles riesgos en cascada, los tipos de amenaza y se analiza la causa-efecto probable de la concentración de riesgos y su correlación?					x	4
18	¿Se entiende como las capacidades de TI contribuyen a la capacidad de la empresa para añadir valor y soportar la pérdida?				x		3
19	¿Se analiza la percepción de la gerencia de la importancia de las capacidades de TI en su estado actual?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
20	¿Se toma en consideración cómo la estrategia de TI, iniciativas de cambio y requisitos externos (P. Ej.: regulaciones, contratos, normas o estándares industriales, entre otros) pueden afectar el perfil de riesgos?				x		3
21	¿Se identifica donde se concentran las zonas de riesgo, los escenarios, las dependencias, los factores de riesgo y medidas de riesgo que requieren atención para posteriormente ser analizados y desarrollados?			x			2
RG1.2	**Definición de umbrales de tolerancia de riesgo de TI**						
22	¿Se establece la cantidad de riesgos relacionados con TI que esta dispuesto a tolerar para cumplir sus objetivos, a nivel de una línea de negocio, producto, servicio, proceso?, ¿se define la propensión o apetito al riesgo a nivel de las diferentes líneas del negocio?				x		3
23	¿Se definen limites en medidas similares a los objetivos del negocio subyacentes y en contra de los impactos del negocio aceptables e inaceptables?			x			2
24	¿Se toman en consideración compensaciones que pueden ser necesarias para alcanzar los objetivos clave en el contexto del equilibrio riesgo/rentabilidad?		x				1
25	¿Se proponen limites y medidas en el contexto de su relación valor/beneficio de implantación de tecnología, programas y ejecución de proyectos de TI, operaciones y ejecución de servicios de TI a través de múltiples horizontes de tiempo (P. Ej.; de inmediato, corto plazo, largo plazo)?				x		3
RG1.3	**Aprobación de niveles de tolerancia al riesgo**						
26	¿Se evalúan las propuestas de umbrales de tolerancia de riesgos contra los riesgos aceptables de la empresa y niveles de oportunidad?		x				1
27	¿Se toman en consideración los resultados de la evaluación de riesgos de TI en la empresa y las compensaciones necesarias para alcanzar los objetivos clave en el contexto del equilibrio riesgo/rentabilidad?				x		3
28	¿Se toma en consideración la concentración de riesgos de TI y la correlación entre las líneas del negocio, productos, servicios y procesos?				x		3
29	¿Se evalúan los umbrales específicos de una unidad para para determinar si estos deben aplicarse a todas las líneas del negocio?			x			2
30	¿Son definidos aquellos tipos de eventos (internos o externos) y cambios en los entornos del negocio o tecnologías, que pueden requerir una modificación a los niveles de tolerancia al riesgo de TI?				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
31	¿Son aprobados los umbrales de tolerancia al riesgo de TI por responsables de la gestión de riesgos?		x				1
RG1.4	**Alineación de la política de riesgos de TI**						
32	¿Se incluye el apetito al riesgo y la tolerancia en la política del riesgo tecnológico a todos los niveles de la empresa?				x		3
33	¿Se reconoce que el riesgo tecnológico es inherente a los objetivos de la empresa y se documenta cuanto riesgo esta dispuesta a asumir (niveles de tolerancia) en búsqueda de lograr los objetivos?				x		3
34	¿Son documentados los principios de gestión de riesgos, las áreas de enfoque de riesgos y las mediciones clave?		x				1
35	¿Se ajusta la política de riesgos de TI basada en los cambios de las condiciones de riesgo y las amenazas emergentes?					x	4
36	¿Se encuentra alineada la política operacional y normas o estándares con la tolerancia al riesgo?		x				1
37	¿Se realizan revisiones periódicas o provocadas, de la política operacional y normas o estándares contra la política de riesgos de TI y la tolerancia?			x			2
38	¿Al identificar brechas, se establecen objetivos definiendo fechas basados en los limites de tiempo de exposición al riesgo aceptables y los recursos necesarios?				x		3
39	niveles de tolerancia de riesgos en lugar de modificar la política operacional y estándares o normas establecidas?				x		3
RG1.5	**Cultura consciente de riesgos de TI**						
40	¿Se promueve una cultura de riesgo capacitando a la empresa para identificar riesgos de TI de forma proactiva, oportunidades e impactos potenciales en el negocio?	x					0
41	¿Los empleados son estimulados para hacer frente a problemas originados por riesgos de TI antes de que estos aumenten gravemente?		x				1
42	¿Se entrena al personal del negocio y de TI acerca de las amenazas, impacto y como reaccionar empleando respuestas planificadas ante eventos de riesgo específicos?			x			2
43	¿Se comunica a las ares enfocadas al riesgo "el porqué debe cuidarse" y se explica como tomar acciones conscientes, de los riesgos no especificados en la política de riesgos?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
44	¿Se realizan ensayos de escenarios para áreas que no se encuentran cubiertas por la política de riesgos de TI y así reforzar las expectativas para la comprender la dirección de la política general y el uso del sentido común?	x					0
45	¿Se fomenta el debate para definir la cantidad apropiada de riesgo a aceptar por parte de la empresa?	x					0
46	¿Se promueve una cultura de gestión de riesgos tecnológicos alineada a la cultura de concientización de riesgos del negocio?	x					0
RG1.6	**Comunicación efectiva de riesgos de TI**						
47	¿Se establece y mantiene un plan de comunicación de riesgos que cubre la política de riesgos de TI, responsabilidades, rendición de cuentas y el panorama de riesgos? (P. Ej.: las amenazas, los controles, el impacto, causas raíz, decisiones del negocio)		x				1
48	¿Se filtra las características del plan de tal modo que sea claro, conciso, útil y dirigido a la audiencia correcta?			x			2
49	¿Se realiza una comunicación frecuente y periódica entre la gestión de TI y la dirección del negocio para tratar la situación actual de riesgos de TI, las preocupaciones o intereses y la exposiciones?			x			2
50	¿Se fomenta una comunicación y administración de TI con un enfoque que busca alinear los riesgos de TI con los riesgos del negocio?		x				1
51	¿Se fomenta una comunicación y administración de TI con un enfoque que busca priorizar periódicamente los riesgos de TI alineados a los riesgos del negocio?			x			2
52	¿Se fomenta una comunicación y administración de TI con un enfoque que busca expresar los riesgos de TI en términos estratégicos y operativos del negocio?				x		3
53	¿Se comunica claramente como los acontecimientos adversos relacionados con TI afectan los objetivos empresariales? (P. Ej.: objetivos del negocio/cuarto de mando integral, las categorías objetivo de COSO ERM)		x				1
54	¿Se fomenta una comunicación clara para que los altos ejecutivos y directivos de TI comprendan la cantidad real de los riesgos de TI y así puedan asignar los recursos adecuados para responder a riesgos de TI alineados al apetito y tolerancia definidos?			x			2
GOBIERNO DE RIESGOS: Integración con ERM							
RG2.1	**Definición y mantenimiento de responsabilidades de gestión de riesgos de TI**						
55	¿Se tienen identificados los responsables y encargados de la gestión de riesgos de TI en toda la empresa?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
56	¿A nivel de los altos ejecutivos y responsables de la gestión de riesgos de TI, se tienen establecidas las expectativas de incorporar la conciencia de riesgos a la cultura organizacional?			x			2
57	¿Se tienen definidas los indicadores de desempeño y procesos de presentación de informes con los niveles adecuados de reconocimiento, aprobación, incentivos y sanciones?				x		3
58	¿Existen estructuras definidas para involucrar al negocio en la toma de decisiones de riesgo-retorno-concientización y de las operaciones del día a día? (P. Ej.: Comité de riesgos del negocio, consejo de riesgos de TI, Oficial de riesgos de TI)			x			2
59	¿Se tienen definidas las funciones que diferencien las responsabilidades de las unidades de negocio (que poseen y gestión del riesgo en el día a día), control interno (que proveen expertos en la materia para evaluación y asesoramiento) y auditoria interna (que ofrecen una garantía independiente)				x		3
60	¿Se tienen definidos los gerentes o directores del negocio con autoridad para tomar decisiones sobre riesgos de TI, beneficios y generación de valor por medio de las TI, programas y ejecución de proyectos de TI, así como operaciones y entrega de servicios de TI?		x				1
61	¿Se tienen definidas las expectativas para los administradores de las políticas, estándares o normas, controles y actividades de supervisión del cumplimiento (P. Ej.: Establecimiento y seguimiento de KRIs)	x					0
62	¿Se establece y evalúa las metas de desempeño para evaluar el equilibrio del riesgo-retorno-concientización en la toma de decisiones? (P. Ej.: la capacidad de los administradores para integrar y equilibrar la gestión del desempeño con la gestión de riesgos a través de sus limites de autoridad)		x				1
63	¿Se tienen roles definidos para administrar dominios específicos de riesgos de TI? (P. Ej.: gestión de la capacidad de los sistemas, dotación personal de TI, selección y evaluación de sistemas o programas)			x			2
64	¿Se asigna a cada dominio un nivel de criticidad en función del riesgo/recompensa o beneficio?	x					0
65	¿De ser necesario, se asignan responsabilidades adicionales para la gestión de riesgos en niveles inferiores o requisitos externos? (P. Ej. Para sistemas específicos)		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
RG2.2	**Coordinación de la estrategia de riesgos de TI y riesgos empresariales**						
66	¿La definición de la gestión de riesgos de TI se realiza en el contexto de la protección y mantenimiento de procesos de negocio o actividades empresariales?				x		3
67	¿El marco de riesgos de TI es alineado al marco existente para la gestión de riesgos del negocio?			x			2
68	¿Los aspectos o información especifica de TI, son integrados en un enfoque empresarial?				x		3
69	¿Se tienen claras las metas y objetivos de riesgos empresariales así como la combinación de factores de riesgos que afectan a la empresa y las limitaciones de recursos?		x				1
70	¿Se define como debe abordarse la gestión de riesgos de TI en el contexto del ámbito de riesgos del negocio y otro tipo de riesgos empresariales?		x				1
71	¿Se tiene definido el papel del departamento de TI en la gestión del riesgo operacional, en función del grado de dependencia del negocio en TI y la infraestructura física, relacionada con el logro de objetivos financieros, operativos y satisfacción del cliente?			x			2
72	¿Se coordinan actividades de evaluación de riesgos y se presentan informes integrados?	x					0
73	¿Los riesgos son clasificados, cuentan con escalas de calificación (p. ej.: frecuencia, magnitud e impacto), categorías de control (p. ej.: predictivo, defectivo o correctivo) y tienen definidas jerarquías en función de políticas de riesgos, estándares o normas y, procedimientos operativos?			x			2
74	¿Cuándo es posible, se emplean principios de ERM y puntos de vistas de riesgos existentes para la gestión del riesgo de TI? (p. ej.: desde el punto de vista actuarial, de cartera, de sistemas)	x					0
75	¿Se evalúa como y cuando ciertos puntos de vista de riesgos del negocio pueden utilizarse para la gestión de riesgos de TI?	x					0
76	¿La estrategia de gestión de riesgos de TI satisface las necesidades unidas de rendimiento de la empresa y requerimientos externos?			x			2

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
RG2.3	**Adaptación de prácticas de gestión de riesgos de TI a prácticas de gestión de riesgo empresarial**						
77	¿Los riesgos existentes son organizados para entender el contexto del negocio de TI (p. ej.: actividades del negocio de TI, análisis de dependencias, análisis de escenarios), identificar los riesgos de TI (p. ej.: modelos de datos, rutas de ajuste o escalamiento), regular los riesgos de TI (p. ej.: procedimientos empresariales de evaluación de riesgos de TI, modelos de decisión en función del riesgo) y gestionar los riesgos de TI (p. ej.: selección de los RISK adecuados para el desempeño de los objetivos del negocio y definir procedimientos de escalamiento)?		x				1
78	¿Se comprenden las expectativas empresariales de la gestión de riesgos, actividades y métodos que son relevantes para la gestión de riesgos de TI? (p. ej.: gestión de problemas, comunicación y formación, como se miden e identifican los riesgos, como se evalúan los controles, que información se proporciona y a quien, como se establece y acuerda el apetito de riesgo)				x		3
79	¿Se evalúan las practicas de gestión de riesgos de TI para identificar brechas a minimizar para satisfacer las expectativas de la ERM?		x				1
80	¿Se identifican las actividades de la gestión de riesgos del negocio que deben agregarse o modificarse para alinearse a la gestión de riesgos de TI?		x				1
81	¿Continuamente se analizan que otras funciones se realizan o deben realizarse en apoyo del cumplimiento de los objetivos del negocio y la gestión de riesgos de TI?		x				1
82	¿Se priorizan y da seguimiento a los esfuerzos que se realizan para cerrar las brechas entre la gestión de riesgos de TI y ERM para mejorar la eficacia y eficiencia (p. ej.: optimizar controles, agilizar las evaluaciones de riesgos, coordinar RISK, escalar desencadenadores, integración de informes)		x				1
RG2.4	**Recursos para la gestión de riesgos de TI**						
83	¿Se analizan las necesidades de recursos para la gestión de riesgos, a nivel de TI como del negocio en el contexto de competencias, aspectos del negocio, limitaciones de recursos y objetivos?			x			2
84	¿Se asignan los fondos necesarios para cerrar las brechas y posicionar a la empresa para tomar ventaja competitiva de las oportunidades?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
85	¿Se evalúa la criticidad del riesgo para intercambiar riesgo/beneficios de acuerdo a los objetivos organizacionales? (p.ej.: asignar más o menos recursos en base a la criticidad de los datos dentro de un procedimiento por etapas para seguridad informática)			x			2
RG2.5	**Aseguramiento independiente de la gestión de riesgos de TI**						
86	¿Se supervisan los riesgos y se establecen planes de acción para garantizar el desempeño de las prácticas realizadas para la gestión de riesgos de TI y, se evalúa si estos se gestionan de acuerdo al apetito y tolerancia al riesgo?		x				1
GOBIERNO DE RIESGOS: Toma de decisiones del negocio considerando los riesgos de TI							
RG3.1	**Gestión ganancia buy-in para el enfoque de análisis de riesgos de TI**						
87	¿Los tomadores de decisiones son formados (instruidos o capacitados) en el enfoque de análisis de riesgos de TI?			x			2
88	¿Se da a conocer como los resultados del análisis de riesgos puede beneficiar las decisiones importantes de la empresa?		x				1
89	¿Se define el nivel de calidad que se espera de los tomadores de decisiones, como interpretar los informes de análisis de riesgos, la definición de términos clave (p. ej.: las probabilidades de riesgo, el grado de error, los factores de riesgo), las limitaciones de las mediciones y las estimaciones basadas en datos incompletos?			x			2
90	¿Se tienen identificadas las brechas del enfoque de análisis de riesgos con las expectativas del riesgo empresarial?		x				1
RG3.2	**Aprobación del análisis de riesgos de TI**						
91	¿Se analizan los informes de riesgos para determinar si estos proporcionan información útil para comprender los riesgos y de ser necesario, para evaluar las opciones de respuesta a los riesgos?			x			2
92	¿Para aprobar el análisis de riesgos TI, se toma en cuenta las limitaciones que se tienen?					x	4
93	¿Los informes presentados de riesgos de TI, son analizados para que estos sean aprobados o rechazado?					x	4
RG3.3	**Incorporación de riesgos de TI en la toma de decisiones estratégicas del negocio**						
94	¿Regularmente se realiza un análisis de los factores de riesgo de TI previo a la toma de decisiones del negocio para que estos sean tomados en cuenta?				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
95	¿Se realiza un análisis del portafolio de aplicaciones en comparación con el valor que ofrecen los procesos del negocio para identificar oportunidades de mejora que tomen en consideración los riesgos, retorno y cambios previstos en el entorno de TI?				x		3
96	¿Se toma en consideración los efectos que tendrá en la gestión empresarial los riesgos de TI y la capacidad de la gestión de riesgos (controles, recursos, capacidades) sobre las decisiones empresariales y del negocio?				x		3
97	¿Como parte de la gestión empresarial, los riesgos de TI son comprendidos desde diversos puntos de vista del portafolio de servicios (p. ej.: unidades del negocio, producto, procesos) y se valora el impacto que tendrá la propuesta de inversión de TI sobre el perfil de riesgos del negocio (reducción o incremento del riesgo)?				x		3
98	¿Para aprobar una decisión del negocio, como condición, el costo y oportunidades se sopesan frente al cambio estimado a la exposición al riesgo de TI?					x	4
RG3.4	**Aceptación de riesgos de TI**						
99	¿Se utilizan umbrales de tolerancia como guía para decidir si se aceptan el nivel de exposición a riesgos restantes?			x			2
100	¿Se realizan evaluaciones de riesgos y se toma en consideración la información pertinente de los informes de análisis de riesgo, tales como las probabilidades de pérdida y los rangos, las opciones de respuesta al riesgo, las expectativas de costo / beneficio, y los posibles efectos de agregación de riesgos?				x		3
101	¿Se realizan análisis con los propietarios de procesos del negocio para examinar la relación riesgo/beneficio y así determinar donde gastar el presupuesto de riesgos de los riesgos "conocidos" para permitir la aceptación del riesgo desconocido?					x	4
102	¿Se definen acuerdos comerciales de aceptación de riesgos o, de no ser aceptables, los requisitos de respuesta a los riesgos correspondientes?				x		3
103	¿Se documenta cuando se toma una decisión de considerar un riesgo fuera de los umbrales de tolerancia justificando la decisión (p. ej.: una importante oportunidad estratégica del negocio)					x	4

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
104	¿Las decisiones de aceptación de riesgos y los requisitos de respuesta a riesgos son comunicados a través de las líneas organizacionales según los riesgos empresariales establecidos, políticas de gobierno corporativo y procedimientos?				x		3
RG3.5	**Priorización de actividades de respuesta al riesgo de TI**						
105	¿Las actividades de respuesta al riesgo son evaluadas para identificar las que tienen mayor probabilidad de impacto sobre la reducción del riesgo total?					x	4
106	¿Se cuantifican los efectos esperados en relación a la frecuencia y la probable magnitud de los escenarios de riesgo a través de la aplicación planificada de controles, capacidades y recursos?			x			2
107	¿Se definen proyectos para la gestión de riesgos con énfasis en la reducción de concentración del riesgo (p. ej.: mejoras en arquitectura), implementación de controles que abarquen varios tipos de riesgos y que sean rentables, implementación de controles que mejoran la eficacia de los procesos y evitan la excesiva toma de riesgos?				x		3
108	¿Se documentan la razón fundamental de la respuesta a riesgos de TI, las limitaciones y cómo la decisión está impulsando cambios en la política publica, controles operativos, capacidades, los despliegues de recursos y planes de comunicación?					x	4
109	¿Para los casos que aplica, se documenta las causas por las cuales se excede o queda por debajo del apetito al riesgo y la tolerancia?				x		3
EVALUACIÓN DE RIESGOS: Recolección de datos							
RE1.1	**Definir y mantener un modelo para recolección de datos e información**						
110	¿Se tiene definido un modelo para la recolección y clasificación y análisis de datos relacionados a los riesgos de TI?				x		3
111	¿En el proceso de recolección de datos se toman en consideración múltiples tipos de eventos (p. ej.: eventos de amenaza, vulnerabilidad o perdida) y múltiples categorías de riesgos de TI (beneficio/valor de habilitación de tecnología, programa y ejecución de proyectos de TI, operaciones y entrega de servicios de TI)?					x	4
112	¿Durante el proceso de recolección de información se toma en consideración filtros y puntos de vista para ayudar a determinar como factores de riesgos específicos pueden afectar al riesgo? (p. ej.: frecuencia, magnitud, impacto en el negocio)				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
113	¿El modelo de recolección de información permite apoyar la medición y evaluación de los atributos de los riesgos (como disponibilidad) a través de los dominios de riesgos de TI y proporciona información útil para establecer incentivos que permitan fomentar una cultura de concientización de riesgos?				x		3
RE1.2	**Recolección de datos sobre el entorno operativo**						
114	¿El modelo de recolección de datos toma en consideración el registro de información sobre el entorno operativo de la empresa para determinar su importancia dentro de la gestión de TI?					x	4
115	¿Para recolectar información del entorno operativo se toman en consideración fuentes dentro de la empresa, departamento legal, auditoria, de cumplimiento y la oficina del CIO?				x		3
116	¿La recolección e información toma en consideración las principales fuentes de ingresos, los sistemas externos, la responsabilidad del producto, el panorama normativo, la competencia en la industria, las nuevas tendencias en la alineación de los competidores con puntos de referencia fundamentales, la madurez relativa de los principales negocios y capacidades de TI y los problemas geopolíticos?					x	4
117	¿La recolección de información toma en consideración datos históricos, riesgos de TI, experiencias de colegas en la industria, bases de datos y acuerdos de la industria para divulgación de eventos comunes (p. ej.: los acuerdos del sector bancario que deben publicar información de los acontecimientos de fraude)?					x	4
RE1.3	**Recolección de datos sobre eventos de riesgos**						
118	¿La recolección de datos sobre eventos de riesgos se realiza considerando eventos que han provocado o pueden provocar impacto en la generación de beneficio/valor de TI, programas, ejecución de proyectos y servicios u operaciones de TI?				x		3
119	¿La recolección de datos sobre eventos de riesgos captura datos relevantes de temas relacionados, incidentes, problemas e investigaciones?					x	4
RE1.4	**Identificación de factores de riesgos**						
120	¿Se identifican factores de riesgo analizando eventos similares para el negocio, organizando los datos y resaltando los factores que contribuyen (p. ej.: los impulsores de la frecuencia y magnitud de los eventos de riesgo)?				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
121	¿Se realizan análisis para determinar que condiciones especificas existían al momento de registrarse los eventos de riesgo y como estas condiciones pudieron haber afectado la frecuencia y la magnitud de la pérdida?			x			2
122	¿Se identifican factores comunes que contribuyen a través de múltiples eventos?			x			2
123	¿Se realizan actividades periódicas y análisis de factores de riesgo para identificar problemas de riesgo nuevos o emergentes y, para comprender de factores de riesgo asociados internos o externos?			x			2
EVALUACIÓN DE RIESGOS: Análisis de Riesgos							
RE2.1	**Definición del alcance de análisis de riesgos**						
124	decidiendo la amplitud y profundidad de las expectativas de los esfuerzos a realizar, tomando en consideración requisitos de decisiones estratégicas (p. ej.: nuevos productos y servicios, nuevos entornos operativos, subcontrataciones, nuevos requisitos de cumplimiento), resultados de evaluaciones empresariales de riesgo de TI, respuestas de indicadores, disparadores o eventos (nuevas o emergentes amenazas); áreas que cuentan con riesgo residual fuera de los umbrales de tolerancia y necesidades de evaluaciones de operaciones en curso?				x		3
125	¿Se cuenta con un mapa de riesgos que involucra factores relevantes de riesgo y la criticidad del negocio en el ámbito de activos/recursos y desencadenadores?	x					0
126	¿La definición del alcance del análisis de riesgos se realiza luego de considerar la criticidad del negocio, los costos de medición contra el valor esperado de la información, la reducción de la inseguridad y cualquier requerimiento regulatorio general?					x	4
RE2.2	**Estimación de riesgos de TI**						
127	¿En todo el ámbito de aplicación del análisis de riesgos de TI, se realiza una estimación de la frecuencia y magnitud probable de la pérdida o ganancia asociada a los escenarios de riesgo de TI, así como la influencia de los factores de riesgo?			x			2
128	¿Al estimar los riesgos, se realiza una estimación de la cantidad máxima de daño que puede tolerar la empresa (p. ej.: una perdida en el peor de los casos se da cuando los factores de riesgo llegan a converger), así como la oportunidad que podría obtenerse?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
129	¿Durante la estimación de riesgos, son considerados escenarios en cascada o coincidencias (p. ej.: una amenaza externa más un accidente interno)?			x			2
130	¿Durante la estimación de riesgos, se desarrollan las expectativas de los controles específicos, capacidad de detección y medidas de respuesta tomando como base los escenarios de riesgo más importantes?.			x			2
131	¿Al estimar los riesgos, se realizan evaluaciones de los controles operativos y sus probables efectos sobre la frecuencia, magnitud y factores de riesgo aplicables?			x			2
132	¿Se realizan estimaciones de los niveles de exposición a riesgos residuales y se compara con la tolerancia aceptable al riesgo para identificar exposiciones que pueden requerir una respuesta al riesgo?	x					0
RE2.3	**Identificar opciones de respuestas a riesgos de TI**						
133	¿Por riesgo identificado, se evalúan las opciones de respuesta al riesgo a tomar como: evitar, reducir/mitigar, transferir/compartir, aceptar o explorar/aprovechar?					x	4
134	¿Se documenta las posibles respuestas al riesgo (soluciones) y se justifican en toda la gama de riesgos?					x	4
135	¿Se definen proyectos o programas de respuesta al riesgo considerando la tolerancia al riesgo, niveles aceptables de mitigación, costos, beneficios y responsabilidades de ejecución?				x		3
136	¿Se establecen requisitos y expectativa para controles materiales en puntos adecuados o donde se espera que se extenderán los riesgos para dar una visibilidad útil?				x		3
RE2.4	**Revisión por pares del análisis de riesgos**						
137	¿El análisis de riesgos de TI es documentado en funciones de las necesidades del negocio?					x	4
138	¿Los estimadores humanos para los controles son calibrados apropiadamente, previo a buscar evidencias de tal forma que no estén orientados a un resultado esperado?				x		3
139	¿El recurso que se asigna para análisis de riesgos de TI cuenta con experiencia, capacidad y el perfil de acuerdo al alcance y complejidad de la revisión de riesgos?				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
140	¿Se evalúan los resultados de las evaluaciones de riesgos de TI, determinando si se logran los objetivos de reducción de riesgo y si el valor de la información obtenida supera los costos de le medición?				x		3
EVALUACIÓN DE RIESGOS: Mantenimiento del Perfil de Riesgos							
RE3.1	**Mapeo de recursos de TI contra procesos del negocio**						
141	¿Se cuenta con un mapa de recursos para procesos de negocio y se mantiene actualizado?			x			2
142	¿El mapa de recursos incluye procesos de negocio, personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y subcontratistas?			x			2
143	¿Se tiene clara la dependencia de las actividades del negocio en los procesos de gestión de servicios de TI y recursos de infraestructura de TI (p. ej.: aplicaciones middleware, servidores, almacenamiento, redes e instalaciones físicas)?					x	4
RE3.2	**Determinar la criticidad del negocio de los recursos de TI**						
144	¿Se tiene identificado que servicios de TI y recursos de TI son necesarios para mantener el funcionamiento de los servicios y procesos clave (críticos) del negocio?					x	4
145	¿Se realizan análisis de dependencias y vínculos débiles para determinar la criticidad del negocio de los recursos de TI, partiendo de la capa de arriba hacia abajo, a las instalaciones físicas?			x			2
146	¿Se consensua con el negocio y la dirección de TI sobre la información más valiosa de la empresa y los activos relacionados con la tecnología? (p. ej.: los utilizados para gestionar operaciones del negocio, proporcionar capacidades, generar valor, proporcionar una ventaja competitiva, proteger los datos empresariales de la rotación del personal, administrar los propósitos y las decisiones de la dirección ejecutiva)				x		3
RE3.3	**Entender las capacidades de TI**						
147	¿Se cuenta con un inventario y se evalúa las capacidades de TI, las habilidades y conocimientos del personal y el resultado del desempeño de todo lo relacionado a la gestión de riesgos (p. ej.: generación de beneficio/valor de TI, programas, ejecución de proyectos y servicios u operaciones de TI)				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
148	¿Se evalúa donde la ejecución normal de los procesos puede o no puede proporcionar los controles adecuados y la capacidad de asumir riesgos aceptables? (p. ej.: no contar con la capacidad de ejecución de proyectos de TI en áreas especificas, sin embargo se cuenta con una solida gestión de programas de TI y la capacidad de contrataciones externas; por lo tanto, se subcontrata en ciertos casos)			x			2
149	¿Se busca constantemente reducir la variabilidad de resultados en los procesos para mejorar la estructura de control interno, mejorar la información y rendimiento del negocio y TI, y explorar/aprovechar las oportunidades?					x	4
RE3.4	**Actualización de los componentes de escenarios de riesgos de TI**						
150	¿para mantener actualizados los componentes de escenarios de riesgos de TI, se realizan evaluaciones periódicas de la colección de atributos a valores a través de escenarios de riesgos de IT y sus conexiones inherentes a las categorías de impacto en el negocio?		x				1
151	¿Se ajustan las entradas de escenarios de riesgo basadas en los cambios de las condiciones de riesgos y amenazas emergentes para generar beneficio/valor de TI, programas, ejecución de proyectos y servicios u operaciones de TI?			x			2
152	¿Se actualizan las distribuciones y rangos componentes de escenarios de riesgos basados en la criticidad de activos/recursos, información sobre el entorno operativo, datos de eventos de riesgos (p. ej.: análisis de causas y tendencias de perdida, problemas en tiempo real y pérdida de datos), datos históricos de riesgos de TI y efectos de factores potenciales de riesgo (p. ej.: influencia en la frecuencia y/o magnitud de los escenarios de riesgo de TI y su impacto potencial en el negocio)?			x			2
153	¿La actualización de escenarios de riesgo incluye la vinculación de tipos de eventos (por categoría, sector de negocio y área funcional) a las categorías de riesgo y categorías de impacto en el negocio?			x			2
154	¿Se actualizan los componentes de escenarios de riesgo de TI en respuesta a cualquier cambio interno o externo considerado como significativo y es revisado periódicamente con un margen mínimo de un año?			x			2

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
RE3.5	**Mantener el perfil de riesgos de TI y el mapa de riesgos de TI**						
155	¿Se utilizan herramientas para mantener el perfil de riesgos como registros de riesgos de TI y un mapa de riesgos?		x				1
156	¿El perfil de riesgos es construido a partir de la evaluación de riesgos del negocio relacionados a TI, componentes de escenarios de riesgos, datos recopilados de eventos de riesgo, análisis de riesgos en curso y resultados de evaluaciones independientes de TI?			x			2
157	¿El proceso de mantenimiento del perfil de riesgos incluye la actualización de atributos clave como el nombre, descripción, propietario, frecuencia esperada y real, la magnitud esperada y real de escenarios de riesgos asociados, el impacto potencial y actual en el negocio, la disposición o acción ante el riesgo (p. ej.: aceptar, transferir, mitigar, evitar)?			x			2
158	¿El mantenimiento del mapa de riesgos incluye la actualización de ponderaciones para cada dimensión? (p. ej.: frecuencia, magnitud, impacto en el negocio, costo para hacer frente al riesgo de acuerdo a la tolerancia aceptable)			x			2
159	¿Se actualiza el mapa de riesgos de TI en respuesta a cualquier cambio interno o externo considerado como significativo y es revisado periódicamente con un margen mínimo de un año?			x			2
RE3.6	**Diseño de indicadores de riesgos de TI**						
160	¿Se definen métricas o indicadores que apuntan a eventos e incidentes relacionados con TI que pueden afectar al negocio?		x				1
161	¿La definición de indicadores se basa en aquello que compromete la exposición y capacidad de gestión de riesgos?		x				1
162	¿Se cuenta con indicadores que alertan cuando la exposición al riesgo supera los umbrales de riesgo aceptables?			x			2
163	¿Se retroalimenta a la dirección para que comprenda la utilidad de los indicadores de riesgo, lo que son, lo cubren, desde la infraestructura a través de una visión estratégica y que acciones tomar si estas se disparan (p. ej.: actualizar el perfil de riesgos, ajustar las actividades de respuesta al riesgo)			x			2
164	¿Se revisan periódicamente los KRIs utilizados por la administración, para recomendar ajustes de acuerdo a los cambios en las condiciones internas y externas?			x			2

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
RESPUESTA A RIESGOS: Articular el riesgo							
RR1.1	**Comunicar los resultados de Análisis de Riesgos**						
165	¿Se retroalimentan los resultados de análisis de riesgos en términos y formatos útiles para apoyar la toma de decisiones del negocio y, en el contexto riesgo-retorno?				x		3
166	¿La comunicación de riesgos incluye la probabilidad de pérdida y/o ganancia, rangos y niveles de confianza que permitan gestionar el balance entre riesgo-rentabilidad?				x		3
167	¿Se identifican y retroalimentan los impactos negativos de eventos y escenarios que debieran impulsar decisiones de respuesta y, los efectos positivos de eventos y escenarios que representan oportunidades que deben canalizarse para evaluar redefinir la estrategia y objetivos?			x			2
168	¿Se provee información a los tomadores de decisiones para comprender los peores escenarios y los más probables; consideraciones legales y regulatorias, exposiciones de una debida diligencia y la importancia de la reputación?			x			2
169	¿La retroalimentación de los resultados incluye componentes claves de riesgo (p. ej.: frecuencia, magnitud, impacto), la magnitud probable de perdida o futura ganancia, escenarios de estimaciones de potenciales perdidas/ganancias y la más probable perdida/ganancia (p. ej.: una frecuencia probable de tres a cinco veces por año y una probable magnitud de perdida entre US$50k y US$100k con un 90% de confianza)?			x			2
RR1.2	**Informe de actividades de la gestión de riesgos de TI y estado de cumplimiento**						
170	¿Se establecen necesidades de información de resultados de gestión de riesgos de TI por las principales áreas interesadas (p. ej.: La junta, comité de riesgos, funciones de control de riesgos, unidades del negocio)?		x				1
171	¿Para presentar información estratégica y eficiente en materia de riesgos de TI y la situación actual, se aplican principios de pertinencia, eficiencia, puntualidad y precisión?			x			2
172	¿Se retroalimenta la eficacia de y rendimiento de la gestión de riesgos, eficacia de los controles, rendimiento de procesos, problemas y carencias, situación actual de remediación, eventos e incidentes y el impacto en el perfil de riesgos?			x			2

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
RR1.3	**Interpretación de resultados de evaluaciones independientes de riesgos de TI**						
173	¿Se revisan y da seguimiento a resultados o hallazgos de terceros objetivos, auditoria interna, control de calidad, autoevaluaciones, entre otras?		x				1
174	¿Los resultados de evaluaciones independientes se mapean al perfil de riesgos, a los riesgos y a la línea base de control, tomando en consideración la tolerancia establecida al riesgo?			x			2
175	¿Se toman en consideración las brechas y las exposiciones del negocio para orientar el objetivo de la gestión de riesgos o establecer necesidades de análisis de riesgos?				x		3
176	¿Se retroalimenta al negocio para que comprenda como los planes de acción correctiva impactan el perfil de riesgos global?			x			2
177	¿Se evalúan los resultados de evaluaciones independientes para identificar oportunidades para la integración con esfuerzos de corrección y otras actividades de gestión de riesgo en curso?				x		3
RR1.4	**Identificar oportunidades relacionadas con TI**						
178	¿En situaciones recurrentes, se consideran los niveles de riesgos de TI para procesos del negocio relacionados a la capacidad de gestión de riesgos de TI, unidades de negocio, productos, etc.?				x		3
179	¿Se evalúan áreas con riesgos relativos y capacidad equivalente de riesgo (es decir, que tienen capacidad de asumir más riesgo) para identificar oportunidades relacionadas con TI que permitan aceptar un riesgo mayor y mejorar el crecimiento y rentabilidad?				x		3
180	¿Se buscan oportunidades donde las TI permitan apalancamiento empresarial, reducción de gastos de coordinación de la empresa, aprovechar las economías de escala y alcance de ciertos recursos comunes a varias líneas de negocio, aprovechar las diferencias estructurales con competidores y coordinar actividades entre las unidades del negocio o en la cadena de valor?					x	4
RESPUESTA A RIESGOS: Gestión del riesgo de TI							
RR2.1	**Inventario de Controles**						
181	¿Se cuenta con un inventario de controles establecidos para la gestión de riesgos y riesgos ha tomarse de acuerdo al apetito al riesgo y su tolerancia?				x		3
182	¿Los controles de riesgos se encuentran clasificados (p. ej.: predictivo, preventivo, detectivo, correctivo) y se encuentran mapeados a riesgos específicos de TI y agrupaciones de riesgos de TI?			x			2

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
183	¿Se diseñan y aplican pruebas periódicas de diseño de controles y pruebas para la eficacia operativa de controles?			x			2
184	¿Se analiza e identifican los procedimientos y la tecnología a utilizar para supervisar el funcionamiento de los controles (por ejemplo, el seguimiento de los controles que intervenga o la automatización de los procesos de supervisión de la empresa)?			x			2
185	¿Se cuenta con una clasificación de controles que incluya las siguientes categorías: Controles desplegados alineados a las expectativas con deficiencias operativas no conocidas, controles alineados a las expectativas con deficiencias operativas conocidas, controles que superan las expectativas con deficiencias operativas no conocidas?			x			2
RR2.2	**Monitorear la alineación operacional de los umbrales de tolerancia al riesgo**						
186	¿Las áreas del negocio aceptan la responsabilidad por operar dentro de sus niveles de tolerancia individual como del portafolio, así como la incorporación de herramientas para supervisar los procesos operativos clave?				x		3
187	¿Se monitorea el rendimiento y eficacia de control así como la variación de los umbrales con los objetivos?	x					0
188	¿Se obtienen compromisos con la dirección sobre los indicadores que funcionaran como KRIS?		x				1
189	¿La implementación de KRIs, establece umbrales, puntos de control (p. ej.: semanal, diario, continuo) y configuraciones de notificaciones (p. ej.: dirección del área del negocio, alta dirección, auditoria interna) de tal forma que los implicados puedan ajustar sus planes de trabajo?		x				1
190	¿Se realizan análisis detallado para determinar zonas de riesgo residuales fuera de los umbrales de tolerancia?			x			2
RR2.3	**Responder a la exposición y oportunidades del riesgo descubiertas**						
191	¿Se hace hincapié en los proyectos para los cuales se espera reducir la frecuencia y magnitud de eventos adversos y pérdidas equilibrando con proyectos que permitan el aprovechamiento de oportunidades estratégicas de negocio?			x			2
192	¿Se fomentan discusiones de análisis de costo/beneficio respecto a la contribución de controles nuevos o existentes que operan dentro de los umbrales de tolerancia de riesgos de TI?				x		3

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
193	¿Se seleccionan controles candidatos de TI basados en amenazas especificas, el grado de exposición al riesgo, la perdida probable y requisitos obligatorios especificados en estándares de TI?				x		3
194	¿Se monitorean los cambios en el perfil de riesgos operativos subyacentes al negocio y se ajusta la clasificación de los proyectos de respuesta a los riesgos?			x			2
RR2.4	**Implementación de controles de riesgos de TI**						
195	¿Se definen los pasos a seguir para garantizar la implementación efectiva de nuevos controles y ajustes a controles existentes?			x			2
196	¿La implementación de nuevos controles de riesgo es comunicada previamente a los interesados clave?					x	4
197	¿Se realizan pruebas piloto de los controles revisando los resultados del rendimiento para garantizar el funcionamiento contra el diseño?					x	4
198	¿Se mapean los nuevos controles operativos y se actualizan los mecanismos de control para medir el rendimiento del control en el tiempo y dar tratamiento inmediato con acciones correctivas cuando sea necesario?				x		3
199	¿Se identifica y capacita al personal sobre los nuevos procedimientos que se han implementado?					x	4
RR2.5	**Informe del progreso del plan de acción de riesgos de TI**						
200	¿Se monitorean los planes de acción de riesgos de TI a todos los niveles para garantizar la eficacia de las acciones necesarias y determinar si se obtuvo la aceptación del riesgo residual?			x			2
201	¿Se garantiza que las acciones realizadas para mitigar el riesgo de TI son propiedad del responsable del proceso afectado y que las desviaciones encontradas son reportadas a la alta dirección?		x				1
RESPUESTA A RIESGOS: Reacción a los acontecimientos							
RR3.1	**Mantenimiento de los planes de respuesta a incidentes**						
202	¿Se documentan los planes de respuesta a amenazas por medio de documentos que describan los pasos a seguir cuando un evento de riesgo puede causar un funcionamiento, desarrollo y/o impacto en la estrategia del negocio (incidentes relacionados con TI) o que ya ha causado un impacto en el negocio?				x		3
203	¿Se mantiene una comunicación abierta sobre la aceptación de riesgos, actividades de gestión de riesgos, técnicas del análisis y los resultados disponibles para ayudar con la preparación del plan de respuesta a riesgos de TI?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
204	¿En la definición de planes de respuesta a incidentes de riesgos de TI, se toma en consideración el tiempo que la empresa puede estar expuesta y cuanto tiempo se tardaría en recuperar si este llegara a materializarse?	x					0
205	¿Basados en el impacto potencial o conocido, se define como debe escalarse en toda la empresa para dar respuesta a un riesgo, desde la gestión del negocio hasta los comités ejecutivos?			x			2
206	¿Se valida que los planes de respuesta a incidentes en procesos críticos, son los adecuados?		x				1
RR3.2	**Supervisión de riesgos de TI**						
207	¿Se monitorea el ambiente para determinar si un control se incumple tomar acciones, ya sea si se escala al siguiente paso de acuerdo al plan de respuesta o se confirma que vuelva a los limites aceptables?		x				1
208	¿Los incidentes son clasificados (p. ej.: perdida de negocio, error del sistema, fraude, demanda) y se compara la exposición real contra los umbrales de tolerancia?	x					0
209	¿Se comunican los impactos comerciales de incidentes a los tomadores de decisiones?			x			2
210	¿Se supervisa que la política de riesgos se cumple y que existe una claridad en las responsabilidades para las acciones de seguimiento?	x					0
RR3.3	**Planes de respuesta a incidentes**						
211	¿Se definen planes de acción para minimizar el impacto de un incidente en curso?	x					0
212	¿Al detectar un incidente, se identifica la categoría para cumplir con los pasos definidos en el plan de respuesta y, se comunica a las partes interesadas y afectadas que ocurre un incidente?			x			2
213	¿Se analiza el incidente y se identifica el tiempo necesario para llevar a acabo el plan de respuesta haciendo los ajustes según corresponda a la situación en curso, asegurando que se adopta la medida correcta?			x			2
RR3.4	**Comunicación de lecciones aprendidas de eventos de riesgo**						
214	¿Se evalúan los anteriores eventos adversos, perdidas y oportunidades de perdida para determinar si hubo una falla derivada de la falta de conciencia, capacidad o motivación?		x				1

Continuación de la encuesta.

	Criterio Evaluación Frecuencia	Frecuencia					
		Nunca	Rara vez	A Veces	Frecuentemente	Siempre	Score
215	¿Se buscan causas raíz de los eventos de riesgo similares y la eficacia de las acciones tomadas antes y ahora para determinar comportamientos y el alcance de problemas subyacentes (p. ej.: problemas sistemáticos graves contra un caso aislado que podría ser gestionado a través de la capacitación del personal o proveer mayor documentación de procedimientos)?		x				1
216	¿Se buscan soluciones tácticas; posibles inversiones en proyectos; o ajustes en el gobierno del riesgo global, la evaluación y/o los procesos de respuesta, para mitigar el riesgo en las operaciones de TI y los incidentes de prestación de servicios relacionados con la oferta de servicios de TI y los niveles de servicio (p. ej.: defectos, reproceso), la integración con la oficina de servicios de TI, el proceso de respuesta a incidentes y el proceso de gestión de problemas de TI; con el objetivo de identificar y corregir la causa subyacente?			x			2
217	¿Se comunica la causa raíz de del problema, los beneficios o valor al negocio, los incidentes en programas de TI y ejecución de proyectos por medio de una comunicación abierta a través de las funciones del negocio y TI?	x					0
218	¿Se comunica la causa raíz, los requisitos adicionales de respuesta al riesgo y las mejoras en los procesos de riesgo para los procesos de gobierno y toma de decisiones?	x					0

Fuente: elaboración propia.

ANEXOS

Anexo A: Distribución de preguntas por categoría

Criterio evaluación: Cumplimiento de estándares			
ID	**Estándar**	**Listado de preguntas**	**Total de preguntas**
E1	Control	13, 15, 62, 65, 72, 100, 181, 187, 189, 193, 207 y 210	12
E2	Documentación	32, 33, 34, 71, 91, 104, 108, 109, 110, 111, 112, 114, 125, 134, 137, 141, 147, 155, 182, 198, 202 y 211	22
E3	Medición	20, 37, 57, 85, 86, 106, 136, 138, 152, 160, 162, 190, 197, 200 y 208	15
E4	Mejora continua	12, 21, 35, 38, 44, 82, 135, 149, 154, 158, 159, 164, 174, 177, 213, 214 y 215	17
Criterio evaluación: Dimensiones de Risk IT			
ID	**Dominio**	**Listado de preguntas**	**Total de preguntas**
RG	Gobierno de riesgos	De la 10 a la 109	100
RE	Evaluación de riesgos	De la 110 a la 164	55
RR	Respuesta a riesgos	De la 165 a la 218	54
Criterio evaluación: Procesos de Risk IT			
ID	**Proceso**	**Listado de preguntas**	**Total de preguntas**
RG1	Establecer y mantener una visión común de riesgos	De la 10 a la 54	45
RG2	Integración con ERM	De la 55 a la 86	32
RG3	Toma de decisiones de negocio conscientes de los riesgos	De la 87 a la 109	23
RE1	Recolección de datos	De la 110 a la 123	14
RE2	Análisis de riesgos	De la 124 a la 140	17
RE3	Mantenimiento del perfil de riesgos	De la 141 a la 164	24
RR1	Articular riesgos	De la 165 a la 180	16
RR2	Gestionar el riesgo	De la 181 a la 201	21
RR3	Reaccionar a acontecimientos	De la 202 a la 218	17

Continuación de la tabla anexo A.

RR2	Gestionar el riesgo	De la 181 a la 201	21
RR3	Reaccionar a acontecimientos	De la 202 a la 218	17
Criterio evaluación: Criterios generales de administración de riesgos			
ID	**Categoría**	**Listado de preguntas**	**Total de preguntas**
C1	Modelos, planes y procedimientos definidos	13, 32, 34, 110, 111, 112, 113, 114, 135, 156, 204, 205 y 211	13
C2	Gestión de comunicación	40, 43, 46, 47, 48, 49, 50, 51, 52, 53, 54, 78, 87, 88, 104, 108, 163, 165, 171, 176, 189, 192, 196, 201, 203, 209, 212, 217 y 218	29
C3	Apetito al riesgo	10, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 33, 39, 45, 64, 65, 99, 102, 158 y 181	21
C4	Reportes y estadísticas	35, 91, 100, 162 y 172	5
C5	Seguimiento y control	37, 38, 62, 72, 81, 86, 96, 106, 109, 132, 136, 140, 149, 150, 152, 157, 160, 173, 175, 178, 183, 184, 187, 190, 193, 194, 200, 207, 208, 214 y 215	31
C6	Responsabilidad	41, 42, 55, 59, 60, 61, 63, 148, 186, 199 y 210	11
C7	Alineamiento	11, 14, 18, 19, 24, 36, 56, 57, 58, 66, 67, 68, 70, 74, 75, 76, 77, 79, 80, 95, 137, 144, 146, 153, 179, 180 y 188	27

Fuente: elaboración propia.

Anexo B.1: Puntuación cumplimiento de estándares

ID	Categoría	Descripción	Score
E1	Control	Se cuenta con procesos, procedimientos y/o mejores prácticas para el seguimiento y control de riesgos	1
E2	Documentación	Se cuenta con procesos, procedimientos y políticas definidas para generar documentación de la gestión de riesgos	3
E3	Medición	Se cuenta con procesos, procedimientos, políticas definidas para la medición del desempeño de la gestión de riesgos	2

Continuación de la tabla anexo B.1.

E4	Mejora continua	Se cuenta con procesos, procedimientos y políticas definidas para gestionar la mejora continua en la gestión de riesgos	2

Fuente: elaboración propia.

Anexo B.2: Puntuación ejecución proceso Framework Risk IT

ID	Proceso	Descripción	Score
RG1	Establecer y mantener una visión común de riesgos	Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la empresa de TI relacionados con la pérdida de liderazgo y la tolerancia subjetiva de ella	2
RG2	Integración con ERM	Integrar la estrategia y las operaciones de gestión de riesgos de TI con las decisiones estratégicas de riesgo de negocio que se han tomado a nivel de empresa	1
RG3	Toma de decisiones de negocio conscientes de los riesgos	Asegurar que las decisiones de la organización toman en cuenta la amplia gama de oportunidades y consecuencias generadas de la dependencia de la TI, para el éxito	3
RE1	Recolección de datos	Identificar los datos pertinentes para hacer viable la identificación de riesgos de TI relacionados, el análisis y presentación de informes	3
RE2	Análisis de riesgos	Desarrollar una información útil para apoyar las decisiones de riesgo que tenga en cuenta la importancia de factores de riesgo de negocios	3
RE3	Mantenimiento del perfil de riesgos	Mantener actualizado el inventario completo de los riesgos conocidos y los atributos (por ejemplo, que se espera, la frecuencia de impacto potencial, disposición), los recursos, las capacidades y los controles como se entiende en el contexto de los productos empresariales, servicios y procesos	2
RR1	Articular riesgos	Garantizar que la información sobre el estado real de las exposiciones y las oportunidades relacionadas con TI se pone a disposición en forma oportuna y a las personas adecuadas para una respuesta adecuada	2

Continuación de la tabla anexo B.2.

RR2	Gestionar el riesgo	Garantizar que las medidas para aprovechar las oportunidades estratégicas y reducir los riesgos a un nivel aceptable se gestionan como un portafolio	2
RR3	Reaccionar a acontecimientos	Asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con la TI se activan de forma oportuna y eficaz	1

Fuente: elaboración propia.

Anexo B.3: Puntuación ejecución dominios Framework Risk IT

ID	Dominio	Descripción	Score
RG	Gobierno de riesgos	Asegura que las prácticas de gestión de riesgos de TI se encuentran integradas a la empresa, permitiendo asegurar la rentabilidad ajustando el riesgo óptimo	2
RE	Evaluación de riesgos	El objetivo consiste en asegurar que los riesgos relacionados con TI y las oportunidades, son identificadas, analizadas y se presentan en términos del negocio	3
RR	Respuesta a riesgos	Garantizar que los temas de riesgo relacionados con TI, las oportunidades y los eventos se abordan de una de manera rentable y de acuerdo con las prioridades del negocio	2

Fuente: elaboración propia.

Anexo B.4: Puntuación criterios generales gestión de riesgos

ID	Categoría	Descripción	Score
C1	Modelos, planes y procedimientos definidos	Modelos, planes y procedimientos para la identificación y respuesta al riesgo	2
C2	Gestión de comunicación	Comunicación de la información relacionada con la gestión de riesgos relacionados con las TI, a las personas interesadas	2

Continuación de la tabla anexo B.4.

C3	Apetito al riesgo	Establecer umbrales de exposición al riesgo, identificación de nuevas oportunidades y riesgos positivos que generen beneficios	2
C4	Reportes y estadísticas	Informes de gestión y análisis de riesgos para evaluar y mejorar los controles	3
C5	Seguimiento y control	Análisis de desempeño y supervisión de los controles	2
C6	Responsabilidad	Definición de roles y responsabilidades de las personas interesadas para gestionar los riesgos de TI	2
C7	Alineamiento	Alineamiento a objetivos estratégicos, lenguaje común e integración con ERM	2

Fuente: elaboración propia.

Anexo C: Frecuencia ejecución actividades Framework Risk IT

ID	Actividad	Proceso	Dominio	Score
RG1.1	Realizar Evaluación de riesgos de TI en la empresa	Establecer y mantener una visión común de riesgos	RG	2
RG1.2	Proponer los umbrales de tolerancia de riesgo de TI	Establecer y mantener una visión común de riesgos	RG	2
RG1.3	Aprobar la tolerancia al riesgo	Establecer y mantener una visión común de riesgos	RG	2
RG1.4	Alinear la política de riesgos de TI	Establecer y mantener una visión común de riesgos	RG	3
RG1.5	Promover una cultura consiente de los riesgos de TI	Establecer y mantener una visión común de riesgos	RG	1
RG1.6	Promover una comunicación efectiva de los riesgos de TI	Establecer y mantener una visión común de riesgos	RG	2
RG2.1	Establecer y mantener la responsabilidad de la gestión de riesgos de TI	Integrar con ERM	RG	1
RG2.2	Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial	Integrar con ERM	RG	1
RG2.3	Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa	Integrar con ERM	RG	1
RG2.4	Proporcionar recursos adecuados para la gestión de riesgos	Integrar con ERM	RG	2
RG2.5	Proveer aseguramiento independiente sobre la gestión de riesgos	Integrar con ERM	RG	1

Continuación de la tabla anexo C.

RG3.1	Gestión ganancia buy-in para el enfoque de análisis de riesgos de TI.	Tomar decisiones de negocio conscientes de los riesgos	RG	2
RG3.2	Aprobar el análisis de riesgo de TI	Tomar decisiones de negocio conscientes de los riesgos	RG	3
RG3.3	Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio	Tomar decisiones de negocio conscientes de los riesgos	RG	3
RG3.4	Aceptar los riesgos de TI	Tomar decisiones de negocio conscientes de los riesgos	RG	3
RG3.5	Priorizar actividades de respuesta a los riesgos de TI	Tomar decisiones de negocio conscientes de los riesgos	RG	3
RE1.1	Establecer y mantener un modelo para la recolección de datos	Recopilar datos	RE	3
RE1.2	Recopilar datos sobre el entorno operativo	Recopilar datos	RE	4
RE1.3	Recopilar datos sobre eventos de riesgo	Recopilar datos	RE	4
RE1.4	Identificar factores de riesgo	Recopilar datos	RE	2
RE2.1	Definir el Alcance del Análisis de Riesgos	Analizar los riesgos	RE	2
RE2.2	Estimar los riesgos de TI	Analizar los riesgos	RE	2
RE2.3	Identificar las opciones de respuesta de riesgo	Analizar los riesgos	RE	4
RE2.4	Realizar una revisión por pares del análisis de riesgos de TI	Analizar los riesgos	RE	3
RE3.1	Mapear los recursos de TI contra procesos de negocio	Mantener el perfil de riesgo	RE	3
RE3.2	Determinar la criticidad de negocio de los recursos de TI	Mantener el perfil de riesgo	RE	3
RE3.3	Entender las capacidades de TI	Mantener el perfil de riesgo	RE	3
RE3.4	Actualizar los componentes de los escenarios de riesgos de TI	Mantener el perfil de riesgo	RE	2
RE3.5	Mantener el perfil de riesgos de TI y el mapa de riesgos de TI	Mantener el perfil de riesgo	RE	2
RE3.6	Diseñar indicadores de riesgos de TI	Mantener el perfil de riesgo	RE	2
RR1.1	Comunicar los resultados del análisis de riesgos de TI.	Articular el riesgos	RR	2
RR1.2	Informe de actividades de la gestión de riesgos de TI y el estado de cumplimiento	Articular el riesgos	RR	2
RR1.3	Interpretar los resultados independientes de la evaluación de TI.	Articular el riesgos	RR	2

Continuación de la tabla anexo C.

RR1.4	Identificar oportunidades relacionadas con TI.	Articular el riesgos	RR	3
RR2.1	Inventario de Controles	Gestionar el riesgo	RR	2
RR2.2	Monitorear la alineación operacional de los umbrales de tolerancia al riesgo	Gestionar el riesgo	RR	1
RR2.3	Responder a la exposición y oportunidades del riesgo descubiertas	Gestionar el riesgo	RR	3
RR2.4	Implementar los controles	Gestionar el riesgo	RR	3
RR2.5	Informar el progreso del plan de acción de riesgos de TI	Gestionar el riesgo	RR	2
RR3.1	Mantenimiento a los planes de respuesta a incidentes	Reaccionar a acontecimientos	RR	1
RR3.2	Supervisión de los riesgos de TI	Reaccionar a acontecimientos	RR	1
RR3.3	Iniciar planes de respuesta a incidentes	Reaccionar a acontecimientos	RR	1
RR3.4	Comunicar las lecciones aprendidas de los eventos de riesgos	Reaccionar a acontecimientos	RR	1

Fuente: elaboración propia.

Anexo D: Controles de riesgos sugeridos por ISACA en The Risk IT Practitioner Guide

1. Riesgos en la infraestructura

1.1. Controles para obsolescencia

- Evaluación de las capacidades y rendimientos actuales
- Establecer un plan de adquisición de infraestructura tecnológica a corto, mediano y largo plazo
- Fomentar la estandarización tecnológica
- Establecer la dirección para la planificación tecnológica

- Realizar mantenimiento de infraestructura de forma periódica en cumplimiento de las recomendaciones establecidas por los fabricantes y proveedores

1.2. Controles para el daño o destrucción de la infraestructura de TI

- Establecer medidas de seguridad para prevenir, detectar y mitigar los riesgos asociados a robo, fuego, agua, humo, actos vandálicos entre otros
- Definir procedimientos de seguridad de acceso físico y perimetral estableciendo las áreas restringidas y permisos de acceso por rol del negocio. Deberán incluirse las actividades para gestionar los accesos, autorizarlos, registrarlos y supervisarlos
- Administración de instalaciones físicas. Los controles deberán incluir medidas para el cumplimiento de normas, leyes, regulaciones y reglamentos acerca de la seguridad, salud y normas operativas internas

1.3. Controles para el robo a infraestructura de TI

- Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
- Controles en procedimientos de personal que gestión en el proceso de reclutamiento, haciendo énfasis en plazas criticas, puestos claves o sensibles para la organización
- Controles para la protección de la infraestructura a nivel de hardware y software que almacenen las actividades realizadas y permitan su posterior revisión. Estos deben incluir responsables del control de

componentes de infraestructura sensibles y críticos para la organización, así como actividades de supervisión

1.4. Controles para arquitectura de infraestructura de TI inadecuada

- Establecer directrices para la planificación tecnológica
- Establecer un proceso bidireccional y reciproco que tome en consideración el plan estratégico del negocio, el plan estratégico de tecnología y las capacidades de TI
- Establecer un comité de profesionales con experiencia y conocimientos, responsables de definir lineamientos y proveer conocimientos sobre cómo realizar las implementaciones garantizando resultados sostenibles

1.5. Controles para la instalación y aplicación de cambios en infraestructura de TI

- Establecer un plan de mantenimiento para la infraestructura que incluya la administración de actualizaciones y correcciones
- Establecer un procedimiento de gestión de cambios y garantizar que los cambios o modificaciones se realizan de acuerdo a los procedimientos definidos

2. Riesgos relacionados al personal de TI

2.1. Controles para la ausencia de personal clave de TI

- Crear y mantener un inventario de personal clave que describa sus habilidades y responsabilidades

- Minimizar la dependencia de personas claves por medio de la documentación, intercambio de conocimientos y un plan de sucesión a puestos clave estableciendo el sucesor y las brechas a cubrir en el sucesor para que pueda cubrirlo en periodos de tiempo considerables

2.2. Controles para la falta de habilidades del personal de TI

- Alinear el proceso de reclutamiento a los procedimientos y normas de la organización
- Establecer un inventario de personal y sus habilidades
- Evaluar el desempeño de los colaboradores según sus responsabilidades, objetivos definidos y logros alcanzados
- Mantener una política de mejora continua de las habilidades y competencias de los colaboradores para apoyarles en el cumplimiento de sus funciones y objetivos organizacionales
- Mantener actualizados los manuales o perfiles de puesto de trabajo de TI, las competencias y los requisitos necesarios para cumplir con las funciones de los diferentes roles
- Analizar constantemente la capacidad de TI vs la demanda actual y futura del negocio para identificar las habilidades necesarias para alcanzar los objetivos del negocio y asegurar la disponibilidad en el tiempo que sea necesario

2.3. Controles para la ausencia de personal clave de TI

- Establecer y mantener un inventario de personal y sus habilidades
- Mantener actualizados los manuales o perfiles de puesto de trabajo de TI, las competencias y los requisitos necesarios para cumplir con las funciones de los diferentes roles

- Analizar constantemente la capacidad de TI vs la demanda actual y futura del negocio para identificar las habilidades necesarias para alcanzar los objetivos del negocio y asegurar la disponibilidad en el tiempo que sea necesario

3. Riesgos en la gestión de proyectos de TI

3.1. Controles para el riesgo de proyectos no finalizados

- Establecer un marco de trabajo para la gestión de proyectos que defina los lineamientos y mejores prácticas a cumplir
- Establecer un comité de proyectos que se responsabilice de priorizar los programas de inversión para que se encuentren alineados con la estrategia de la organización
- Elaborar un conjunto de mediciones que permitan evaluar el cumplimiento de objetivos
- Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad

3.2. Controles para riesgo económicos de proyectos

- Establecer procedimientos para la administración de costos ejecutados versus presupuestados para determinar desviaciones, impacto para definir si se asigna más presupuesto o se acepta el costo de oportunidad de no asignarlo
- Establecer procedimientos para la definición de presupuestos de tecnología considerando costos operativos, mantenimiento, actualizaciones, inversión y prioridades definidas

- Establecer métricas de control para el cumplimiento de proyectos enfocados en cumplimiento de tiempos, costos y calidad
- Establecer un comité de proyectos que se responsabilice de priorizar los programas de inversión para que se encuentren alineados con la estrategia de la organización
- Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad

3.3. Controles para riesgo de retraso en la entrega de proyectos

- Establecer métricas de control para el cumplimiento de proyectos enfocados en cumplimiento de tiempos, costos y calidad
- Establecer métricas individuales que midan el desempeño de los recursos asignados a proyectos. Estas deberán proveer información para mejorar la estimación de tiempos de entrega, comparar estadísticas con el mercado y evaluar si es necesario realizar cambios, entrenamiento, balancear cargas de trabajo, modificar procedimientos entre otros
- Establecer un comité de proyectos que se responsabilice de priorizar los programas de inversión para que se encuentren alineados con la estrategia de la organización
- Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad

3.4. Controles para riesgos por baja calidad en los proyectos

- Establecer un marco de trabajo para la gestión de proyectos que defina los lineamientos y mejores prácticas a cumplir
- Implementar procedimientos de aseguramiento de calidad cuyas actividades deben ser parte de los planes de desarrollos de proyectos.
- Establecer un comité de profesionales con experiencia y conocimientos, responsables de definir lineamientos y proveer conocimientos sobre cómo realizar las implementaciones garantizando resultados sostenibles
- Establecer compromisos con los Stakeholders de tal forma que participen en la definición y ejecución de las actividades de proyecto, haciéndolos parte del mismo para aprovechar el conocimiento en los procesos y del negocio
- Fomentar la estandarización tecnológica definiendo normas y estándares para todo el ciclo de vida de proyectos
- Asegurar que los dueños de procesos, personal de tecnología, aseguramiento de calidad e interesados, aprueben el resultado de las pruebas de acuerdo al plan de pruebas establecido
- Certificar que se obtienen los resultados esperados al finalizar los proyectos, informar a los patrocinadores, usuarios y equipo del proyecto documentando las lecciones aprendidas y definiendo planes de acción si no se cumple con los requerimientos del proyecto

3.5. Controles para la falta de visión del portafolio de proyectos

- Establecer un marco de trabajo para la gestión de proyectos que defina los lineamientos y mejores prácticas a cumplir
- Establecer métricas de control para el cumplimiento de proyectos enfocados en cumplimiento de tiempos, costos y calidad

- Establecer un comité de proyectos que se responsabilice de priorizar los programas de inversión para que se encuentren alineados con la estrategia de la organización
- Establecer acuerdos de servicios con indicadores de desempeño que midan el cumplimiento y efectividad, para garantizar el ciclo de mejora continua
- Establecer mediciones para monitorear y evaluar el cumplimiento de objetivos
- Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad

4. Riesgos en la seguridad de TI

4.1. Controles para ataques lógicos

- Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
- Desarrollar y mantener un BCP con instrucciones claras para recuperar los servicios críticos de TI, con responsabilidades y procedimientos de comunicación
- Establecer planes de pruebas periódicas de seguridad, implementar mecanismos de vigilancia, monitoreo y control, que alerten y reporten eventos detectados de traspasos de seguridad
- Establecer mecanismos de prevención, detección y corrección de intromisiones de software malicioso, así como procedimientos de actualizaciones de seguridad y antivirus

- Establecer procedimientos y normas de seguridad de red que incluya técnicas y procesos de asignar o denegar accesos, control de flujos de información, entre otros
- Establecer procedimientos para gestionar la seguridad de información que incluyan la descripción de actividades para recepción, almacenamiento y egreso de datos
- Establecer la cultura de definición de los propietarios de datos, sistemas y procesos por parte de las áreas del negocio responsables de la información

4.2. Controles para el traspaso de seguridad

- Establecer procedimientos para la administración de usuarios, roles y accesos, definiendo procesos claros de autorización, altas, bajas y modificaciones de usuarios
- Garantizar que los usuarios se identifican de forma única e inequívoca por medio de la autenticación para poder acceder a los recursos y servicios y aplicativos
- Proveer y mantener una matriz de perfil de puestos y funciones que identifique el perfil de accesos estándar y permita autorizar y documentar excepciones
- Establecer planes de pruebas periódicas de seguridad, implementar mecanismos de vigilancia, monitoreo y control, que alerten y reporten eventos detectados de traspasos de seguridad
- Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
- Establecer procedimientos que aseguren el conocimiento y compromiso de los usuarios al cumplimiento de las políticas enfocadas a la protección

y uso de los activos de información y recursos tecnológicos de la organización

4.3. Controles para el riesgo de alteración de la integridad de la información

- Establecer la cultura de definición de los propietarios de datos, sistemas y procesos por parte de las áreas del negocio responsables de la información
- Establecer un procedimiento para la gestión de cambios de aplicaciones, procedimientos, procesos, sistemas, configuraciones de componentes de infraestructura de hardware y software, que defina actividades de aprobación, categorización y priorización
- Mantener actualizado el inventario de activos de TI que incluya su tipificación e interrelación
- Definir procedimientos para la generación de respaldos y recuperación de información que permita clasificarla y especifique que información se excluye o incluye, así como los periodos de tiempo en los cuales estarán disponibles

4.4. Controles para la exposición de la información

- Definir la política de traslado de información sensible que especifique que los datos sensibles solo podrán ser trasladados por medios estandarizados autorizados y aprobados por el negocio
- Definir una política del uso de internet, correos electrónicos personales y el uso de dispositivos externos que pueden conectarse a la red interna
- Establecer un procedimiento que garantice que todos los colaboradores tienen conocimiento y se comprometen a cumplir las políticas enfocadas

a la protección de los activos de información y recursos tecnológicos de la organización

- Establecer mecanismos de protección de activos de información en equipos estacionarios y en especial para equipos móviles los cuales presentan una mayor exposición a riesgos

5. Riesgo en aplicaciones de TI

5.1. Controles para decisiones incorrectas de inversión en aplicaciones de TI

- Establecer un comité de proyectos que se responsabilice de priorizar los programas de inversión para que se encuentren alineados con la estrategia de la organización
- Establecer compromisos con los Stakeholders de tal forma que participen en la definición y ejecución de las actividades de proyecto, haciéndolos parte del mismo para aprovechar el conocimiento en los procesos y del negocio
- Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
- Establecer métricas de control para el cumplimiento de proyectos enfocados en cumplimiento de tiempos, costos y calidad
- Analizar constantemente la capacidad de TI vs la demanda actual y futura del negocio para identificar las habilidades necesarias para alcanzar los objetivos del negocio y asegurar la disponibilidad en el tiempo que sea necesario

5.2. Controles para la caducidad de las aplicaciones del negocio

- Fomentar la estandarización tecnológica
- Establecer la dirección para la planificación tecnológica
- Establecer procedimientos para dar mantenimiento a las aplicaciones de software que incluyan evaluaciones periódicas para implementar mejoras en diseño y funcionalidad
- Evaluar la capacidad actual y el rendimiento de las soluciones entregadas y compararlas con las necesidades futuras

5.3. Controles para la implementación inadecuada de aplicaciones

- Implementar dentro de los procedimientos de desarrollo las fases de planificación, la especificación y puntos de control para alcanzar la calidad 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 de proyectos aprobados por los interesados
- Asegurar que los dueños de procesos, personal de tecnología, aseguramiento de calidad e interesados, aprueben el resultado de las pruebas de acuerdo al plan de pruebas establecido

5.4. Controles para el riesgo de inestabilidad de las aplicaciones

- Establecer procedimientos para dar mantenimiento a las aplicaciones de software

- Monitorear periódicamente el rendimiento y la capacidad de las aplicaciones y recursos de TI para asegurar que cumplan con los niveles de servicio acordados con los usuarios y obtener el estado real de las aplicaciones
- Asegurar que los dueños de procesos, personal de tecnología, aseguramiento de calidad e interesados, aprueben el resultado de las pruebas de acuerdo al plan de pruebas establecido
- Establecer un procedimiento para la administración de problemas que permita la trazabilidad de problemas, e incluya información referente al problema como: detalle de errores, causas raíz, recursos afectados, recursos utilizados, tiempos de los eventos y solución aplicada

5.5. Controles para el riesgo de falta de capacidad de las aplicaciones

- Monitorear periódicamente el rendimiento y la capacidad de las aplicaciones y recursos de TI para asegurar que cumplan con los niveles de servicio acordados con los usuarios y obtener el estado real de las aplicaciones
- Realizar mantenimiento de infraestructura de forma periódica en cumplimiento de las recomendaciones establecidas por los fabricantes y proveedores

5.6. Controles para el riesgo de caducidad de aplicaciones de infraestructura

- Establecer la dirección para la planificación tecnológica
- Establecer un plan de adquisición de infraestructura tecnológica a corto, mediano y largo plazo

- Realizar mantenimiento de infraestructura de forma periódica en cumplimiento de las recomendaciones establecidas por los fabricantes y proveedores

5.7. Control para el riesgo de aplicaciones intrusas

- Establecer mecanismos de prevención, detección y corrección de intromisiones de software malicioso, así como procedimientos de actualizaciones de seguridad y antivirus

6. Riesgos en los servicios que provee TI

6.1. Controles para el riesgo en la entrega y soporte de servicios de TI

- Establecer un procedimiento para la selección de proveedores que sea transparente e imparcial, asimismo que incluya la creación, modificación y cancelación de contratos con proveedores
- Establecer una normativa que dicte los lineamientos para establecer acuerdos de servicio con los proveedores y los compromisos que sean adquiridos por ambas partes
- Establecer contratos con proveedores apegados a las normativas internas y legales; clarificar los términos de seguridad, sanciones o penalizaciones y premios
- Establecer un proceso que permita definir y reunir las métricas que midan el cumplimiento de los acuerdos de servicios, incluyendo acuerdos de servicio provistos por los proveedores

6.2. Controles para riesgos de rendimiento de servicios

- Definir los acuerdos de niveles de servicio como mínimo para los que son críticos, basándose en la capacidad de TI y los requisitos de los interesados con quienes deberán acordarse considerando la disponibilidad, fiabilidad, restricciones, seguridad, rendimiento, continuidad y tiempos de respuesta
- Diseñar un plan de recuperación y reanudación de servicios de TI
- Establecer un proceso que permita definir y reunir las métricas que midan el cumplimiento de los acuerdos de servicios, incluyendo acuerdos de servicio provistos por los proveedores
- Desarrollar y mantener un BCP con instrucciones claras para recuperar los servicios críticos de TI, con responsabilidades y procedimientos de comunicación

7. Riesgos en el cumplimiento corporativo de TI

7.1. Controles para riesgos en el cumplimiento de acuerdos y compromisos

- Establecer una normativa que dicte los lineamientos para establecer acuerdos de servicio con los proveedores y los compromisos que sean adquiridos por ambas partes

7.2. Controles para riesgos en el cumplimiento de licenciamiento

- Identificar las regulaciones locales e internacionales referentes a la propiedad intelectual y derechos sobre licenciamiento

- Establecer políticas para prohibir el uso de software sin el licenciamiento y que regule el uso de software libre en la organización

8. Riesgos en el cumplimiento legal de TI (aplicado a Guatemala)

8.1. Controles riesgos en el cumplimiento legal de TI

- Identificar las regulaciones locales e internacionales referentes a normas de la industria, laborales y fiscales que se encuentren relacionadas a las políticas y procedimientos internos de TI
- Establecer derechos de propiedad intelectual internos para el desarrollo de software y programas informáticos por parte del personal de tecnología como parte de sus funciones. Estos deberán quedar estipulados por medio de documentos definido por la organización y aceptado por el personal de tecnología

9. Otros escenarios de riesgos de TI

9.1. Control de riesgos en la rendición de cuentas de TI

- Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión

9.2. Controles de riesgos de integración de TI y procesos de negocio

- Establecer un proceso que fomente la educación y comunicación bidireccional de la planeación estratégica de TI con el negocio

- Establecer un procedimiento y mecanismos que faciliten la coordinación, comunicación e interacción entre el personal de TI y las partes interesadas del negocio

9.3. Controles de riesgos en procesos operativos de TI y de manejo de errores

- Establecer un procedimiento de entrenamiento y capacitación para personal de nuevo ingreso que contemple la formación continua alineada a las funciones de los roles para alcanzar los objetivos organizacionales
- Definir y documentar los procedimientos operacionales de TI
- Diseñar un plan de recuperación y reanudación de servicios de TI