Universidad Nacional de Costa Rica

Sistema de Estudios de Posgrado

Maestría en Tecnologías de la Información (MATI)

Énfasis en Gestión de Proyectos

Manual de buenas prácticas para la gestión de riesgos en tecnologías de la información en organizaciones financieras de carácter local en Costa Rica

Autor(a): Ivannia Rojas Gutiérrez

Heredia, Costa Rica, 26 de noviembre de 2025

MIEMBROS DEL TRIBUNAL EXAMINADOR

Mag. Eduardo Mena Ugalde

Coordinador del posgrado

Máster Harold Leiva Martínez

Tutor de tesis

Máster Xenia Guerrero Arias

Miembro del Comité Asesor

Ivannia Rojas Gutiérrez

Sustentante

UNIVERSIDAD NACIONAL
VICERRECTORÍA DE INVESTIGACIÓN
SISTEMA DE INFORMACIÓN DOCUMENTAL
REPOSITORIO ACADÉMICO INSTITUCIONAL
NOMBRE DE LA INSTANCIA ACADÉMICA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

FORMULARIO DE DEPÓSITO LEGAL, LICENCIA AUTORIZACIÓN DE USO DE DERECHOS PATRIMONIALES DE LA PERSONA AUTORA E INCORPORACIÓN A REPOSITORIOS ACADÉMICOS INSTITUCIONALES DE INFORMACIÓN DE ACCESO PÚBLICO

Por este medio, la(s) persona(s) suscrita(s), abajo firmante, estudiante(s) de la carrera de MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN, y titular(es) del Trabajo Final de Graduación denominado:
Manual de buenas prácticas para la gestión de riesgos en tecnologías de la información en organizaciones financieras de carácter local en Costa Rica en la modalidad Proyecto de graduación para optar al grado académico de MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN, de conformidad con lo establecido en el REGLAMENTO GENERAL DEL PROCESO DE ENSEÑANZA Y APRENDIZAJE DE LA UNIVERSIDAD NACIONAL, ARTICULO 90, relacionada con trabajos finales de graduación, DECLARO BAJO FE DE JURAMENTO conociendo la responsabilidad civil, penal o administrativa en que podría incurrir al no decir la verdad, lo siguiente:

1. Que el documento resultado del Trabajo Final de Graduación ha cumplido con todo el proceso de aprobación, que confiere el grado académico postulado.

2. Autorizo el depósito del Trabajo Final de Graduación en formato digital, en el Repositorio Académico Institucional (RAI) de la Universidad Nacional.

3. Libero de responsabilidad a las autoridades de la Instancia Académica MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN y a las personas funcionarias encargadas de la curación de los metadatos y posterior divulgación de los Trabajos Finales de Graduación en el RAI, en relación con el reconocimiento que se realiza respecto de los niveles de participación asignados por las propias personas autoras del Trabajo Final de Graduación. Esto para casos de Trabajos Finales de Graduación elaborados como obra colaborativa, ya que todas las personas autoras han contribuido intelectualmente en la elaboración del documento.

4. En caso de que el Trabajo Final de Graduación fuese elaborado como obra colaborativa, este formulario debe incluir todas las firmas de las personas autoras, en caso de no incluir alguna firma este no podrá ser compartido en acceso abierto, en concordancia con el artículo 90. (Reglamento general del proceso de enseñanza y aprendizaje de la Universidad Nacional)

5. Permito a las Bibliotecas del Sistema de Información Documental de la Universidad Nacional (SIDUNA) poner a disposición del público los metadatos https://docs.google.com/document/d/1ySIOtQ_uNEKJnNOOoxYdlQof5EPSuUQ2liso8oBD1zg/edit) a través de los espacios de divulgación que posee la Universidad Nacional, a partir del cual las personas usuarias de dichas plataformas puedan acceder a los metadatos y hacer uso de estos en el marco de los fines definidos por las personas autoras en este instrumento con el debido respeto a la integridad del contenido de estos.

6. Concedo a favor de la Universidad Nacional una licencia gratuita, no exclusiva, de ámbito mundial y por plazo indefinido, de la totalidad de los derechos patrimoniales de autor, incluidos pero no limitados a los derechos de utilización, reproducción, publicación, comunicación o disposición pública, distribución, transformación, y en fin, cualquier otra forma de utilización, proceso o sistema conocido o por conocerse, por cualquier medio, sea impreso y/o digital; siempre y cuando, sea única y exclusivamente para efectos culturales, educativos, académicos y ordinarios de la institución, sin fines de lucro. A manera enunciativa y no limitativa, incluye además los siguientes actos

a. La edición gráfica y de estilo del Trabajo Final de Graduación y/o parte de este.

b. La publicación y reproducción íntegra de la obra y/o parte de esta, tanto por medios impresos como electrónicos, en el cual se incluye Internet y cualquier otra tecnología conocida o por conocer.

c. La traducción a cualquier idioma o dialecto del Trabajo Final de Graduación o parte de este.

d. La generación de obras derivadas a partir del documento original, respetando siempre los derechos de autor.

e. La adaptación de la obra a formatos de lectura, sonido, voz y cualquier otra representación o mecanismo técnico disponible, que posibilite su acceso para personas no videntes parcial o totalmente, o con alguna otra forma de capacidades especiales que le impida su acceso a la lectura convencional del Trabajo Final de Graduación.

f. La distribución y puesta a disposición de la obra al público, de tal forma que el público pueda tener acceso a esta desde el momento y lugar que cada uno elija, a través de los mecanismos físicos o electrónicos disponibles.

g. Cualquier otra forma de utilización, proceso o sistema conocido o por conocerse que se relacione con las actividades y fines académicos vinculados a la Instancia Académica MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN y la Biblioteca JOAQUÍN GARCÍA MONGE de la Universidad Nacional.

De acuerdo con lo anterior, autorizo a que mi Trabajo Final de Graduación, se publique, comunique públicamente y se distribuya bajo los lineamientos establecidos por la Universidad Nacional en cuanto al uso de las licencias gratuitas en las publicaciones en acceso abierto
(Creative Commons https://creativecommons.org/choose/?lang=es_es)

7. Acepto que el Trabajo Final de Graduación aportado, sea sometido al proceso de curación de metadatos por personal bibliotecólogo asignado para administrar el RAI de la comunidad de la Biblioteca JOANQUÍN GARCÍA MONGE cuanto a requerimientos bibliográficos. (Normas técnicas de curaduría de metadatos del RAI)

10. Reconozco que la Biblioteca JOAQUÍN GARCÍA MONGE actuara con diligencia para evitar en el Repositorio Académico Institucional (RAI) de la Universidad Nacional, contenidos ilícitos. En caso de identificar o que tenga conocimiento efectivo de la existencia de infracciones a los derechos de propiedad intelectual, se reserva el derecho de proceder a embargar el acceso durante el trámite del debido proceso para comprobar el incumplimiento y en caso de verificarse la falta, retirar definitivamente el acceso al Trabajo Final de Graduación depositado.

11. De conformidad con el artículo 87 del Reglamento general del proceso de enseñanza y aprendizaje de la Universidad Nacional, lo resuelto en la Comisión de Trabajo Final de Graduación, y el Tribunal

Evaluador en la defensa celebrada el día 26 de noviembre de 2025, acepto que se aplique la confidencialidad parcial del TFG según los términos previamente acordados.

Acepto que la divulgación y puesta a disposición al público del Trabajo Final de Graduación, salvo los posibles términos de confidencialidad acordados para cada caso. Así como la presente autorización de uso de la obra, se regirá por la normativa institucional de la Universidad Nacional, Costa Rica y la legislación de la República de Costa Rica. Adicionalmente, en caso de cualquier eventual diferencia de criterio o disputa futura, acepto que esta se dirimirá de acuerdo con los mecanismos de Resolución Alterna de Conflictos y la Jurisdicción Costarricense.

Nombre y apellidos de la persona autora: Ivannia Rojas Gutiérrez

Cédula de identidad: 116860447

Correo electrónico personal: Ivannia.rojas.gutierrez@utlook.com

Nombre de la Instancia Académica: Maestría en Tecnologías de la Información

Fecha de entrega: 26 de noviembre de 2025

Firma:

Como requisito legal, la firma de las personas autoras debe incluir la firma de 2 personas testigos. (NO APLICA PARA LAS FIRMAS EN FORMATO DIGITAL)

Nombre y apellidos de la persona testigo 1: Rosa Rojas Gutiérrez

Cédula de identidad: 116360886

Número telefónico: 86651174

Fecha: 24 de noviembre de 2025

Firma:

Nombre y apellidos de la persona testigo 2: Yenny Gutiérrez Mora

Cédula de identidad: 602990749

Número telefónico: 85641667

Fecha: 24 de noviembre de 2025

Firma: Yenny Gutiérrez Mora

Tabla de contenidos

Índice de Cuadros

Índice de Gráficos

Índice de Figuras

Índice de Anexos

Dedicatoria

A Dios, por darme la fortaleza, la sabiduría y la fe necesarias para culminar este camino.

A mis padres, Yenny y Félix, por ser mis pilares, mi fuerza en los momentos difíciles y mi inspiración constante para nunca rendirme.

A mis hermanos Ethan y Sofía, con el deseo de ser inspiración para que alcancen sus sueños.

A mi familia, por su amor incondicional y por motivarme siempre a seguir adelante.

A mi tutor Harold Leiva Martínez, por su paciencia, orientación y valiosas enseñanzas.

Y a mí misma, por confiar en que la perseverancia convierte los sueños en realidad.

Agradecimientos

Con todo mi corazón, agradezco a quienes
iluminaron mi camino con su apoyo.

Agradezco al Máster Norberto Lee Rodríguez Madrigal,
por su valioso apoyo en la validación de la propuesta de solución.

A mis profesores, por la enseñanza y orientación brindadas
durante todo este proceso.

A mis compañeros de estudio, amigos que hicieron
inolvidable esta trayectoria de aprendizaje.

A la Universidad Nacional, por brindarme las herramientas
y el espacio para crecer profesional y personalmente.

RESUMEN EJECUTIVO

Este documento aborda una necesidad crítica en las entidades financieras locales de Costa Rica, bajo la supervisión de la SUGEF. El diagnóstico realizado reveló que la principal barrera para una gestión de riesgos de TI efectiva no es técnica, sino humana: una marcada resistencia al cambio y una cultura organizacional débil. Por ello, el objetivo de este estudio fue desarrollar un manual de buenas prácticas que transforme esta realidad, elevando el nivel de madurez de la gestión de riesgos de TI a un proceso proactivo, estandarizado y de alto valor estratégico.

La investigación, de enfoque cualitativo y tipo aplicada, se fundamentó en marcos de referencia líderes como COBIT 2019 y parte de los lineamientos de la SUGEF para la gestión del riesgo. Como resultado principal, se estructuró un manual cuyo eje principal es la Gobernanza de TI, del cual se desprenden cuatro dimensiones estratégicas e independientes, diseñadas para superar los obstáculos identificados. Estas dimensiones son: Cultura Organizacional (enfocada en conciencia y capacitación), Comunicación Colaborativa (mejorando la coordinación entre las líneas de defensa), Priorización (a través de un procedimiento estructurado para clasificar riesgos), y la Inteligencia Artificial en la Evaluación Predicitiva.

En esencia, este manual es una lectura esencial para ejecutivos y profesionales del sector financiero. Ofrece no solo una ruta clara hacia el cumplimiento normativo de la SUGEF, sino que, de manera más importante, proporciona una verdadera ventaja competitiva cimentada en la resiliencia tecnológica y una gestión de riesgos de TI de vanguardia.

CAPÍTULO 1. EL PROBLEMA Y SU IMPORTANCIA

Antecedentes

Parte de las organizaciones financieras de carácter local en Costa Rica operan bajo el marco regulatorio y las directrices emitidas por la Superintendencia General de Entidades Financieras (SUGEF), organismo encargado de supervisar y regular entidades financieras. La SUGEF (s.f) tiene como objetivo “contribuir con la estabilidad, fortaleza, eficiencia e integridad del Sistema Financiero Nacional (SFN) para preservar la confianza de la sociedad, aplicando las potestades asignadas por el ordenamiento jurídico”. Esta supervisión incluye la emisión de lineamientos orientados a la gestión de riesgos en el área de Tecnologías de la Información (TI).

Según Ivanova (2021, p. 55), “la inestabilidad del entorno enfrenta a las organizaciones a una serie de factores desconocidos, cuyo impacto deben afrontar”. En el desarrollo de sus actividades, las instituciones se ven expuestas a diversos riesgos que pueden afectar el cumplimiento de los objetivos definidos. Debido a esto, resulta necesario comprender cómo estos riesgos inciden en las instituciones. Por tanto, “la gestión de riesgos es una de las competencias más importantes de los gerentes y equipos de proyectos de TI, ya que les permite anticipar posibles amenazas y riesgos, aumentando así las probabilidades de alcanzar los objetivos planificados” (Nikolaenko & Sidorov, 2023, p. 3).

Dada la importancia de la estabilidad financiera y la confianza de los clientes en estas instituciones, una gestión de riesgos efectiva es esencial para asegurar su sostenibilidad, especialmente en un sector donde la información es un activo valioso. Por ello, las organizaciones financieras deben adoptar buenas prácticas alineadas con las directrices de la SUGEF, con el propósito de fortalecer la gestión en sus procesos. La presente investigación delimita su alcance a la gestión de los riesgos específicos del área de TI.

Justificación

Debido a la naturaleza crítica de sus operaciones y el manejo de información sensible, las organizaciones financieras de carácter local deben implementar un enfoque estructurado de gestión de riesgos que asegure la mitigación de amenazas y el aseguramiento en la confianza de sus clientes. Según Ivanova (2021), la gestión de riesgos debe estar incorporada en la estrategia y la cultura organizacional, de modo que las soluciones definidas a nivel estratégico se transformen en actividades prácticas que el personal pueda entender y llevar a cabo efectivamente. Sin embargo, cuando se presentan puntos débiles en la gestión, las organizaciones se ven expuestas a diversas vulnerabilidades operativas y de cumplimiento.

La elaboración de un manual de buenas prácticas resulta valiosa, ya que proporcionará a las organizaciones un conjunto de pautas claras y detalladas, alineadas con las directrices establecidas por la SUGEF. Finalmente, dicho manual permitirá a los responsables de TI disponer de un recurso práctico que facilite la toma de decisiones informadas y promueva la adopción de medidas proactivas orientadas al fortalecimiento de la gestión de riesgos.

Definición del problema

Las organizaciones financieras de carácter local en Costa Rica presentan una oportunidad de mejora significativa en la gestión de riesgos en TI. Con el tiempo, se han presentado áreas de vulnerabilidad que constituyen riesgos críticos dentro del sector. La iniciativa propone elaborar un manual estructurado que fortalezca estas áreas. Para identificarlas de manera específica, se llevará a cabo un estudio que integrará encuestas, entrevistas y revisión de la literatura.

En consecuencia, el desarrollo e implementación del manual se considera fundamental, al brindar a los responsables del área de TI una guía clara y estructurada destinada a fortalecer la gestión.

Pregunta de investigación

¿Cuáles son las mejores prácticas para la gestión de riesgos en Tecnologías de la Información (TI) para organizaciones financieras de carácter local en Costa Rica, considerando las directrices de la SUGEF?

Objetivo general

Elaborar un manual de buenas prácticas para la gestión de riesgos en Tecnologías de la Información (TI) en organizaciones financieras de carácter local en Costa Rica, a partir del diagnóstico de la situación actual, la revisión de mejores prácticas y el análisis de brechas, con el propósito de fortalecer su capacidad para identificar, evaluar y mitigar riesgos tecnológicos.

Objetivos específicos

1. Realizar un diagnóstico de la situación actual de la gestión de riesgos en el área de TI de las organizaciones financieras locales, mediante una evaluación que permita establecer una línea base para proponer mejoras concretas.

2. Examinar las mejores prácticas en el campo de las tecnologías de la información para la gestión de riesgos en TI, mediante una revisión documental de marcos normativos, estudios de caso y literatura, con el fin de contar con un referente técnico que permita orientar la mejora de la gestión de riesgos en las organizaciones financieras de carácter local.

3. Analizar las brechas entre la situación actual de la gestión de riesgos de las organizaciones financieras de carácter local y las mejores prácticas identificadas, mediante una comparación estructurada entre los hallazgos del diagnóstico y los referentes teóricos y normativos, con el fin de identificar áreas de mejora prioritarias y sustentar las propuestas de intervención.

4. Construir un manual de buenas prácticas para la gestión de riesgos de TI, con base en las brechas detectadas, las mejores prácticas estudiadas y las directrices emitidas por la SUGEF en Costa Rica, con el fin de proporcionar una herramienta práctica que fortalezca la gestión de riesgos en organizaciones financieras de carácter local.

5. Validar el manual de buenas prácticas elaborado, mediante el criterio de expertos del área de TI y gestión de riesgos en el sector financiero, para determinar su impacto potencial, aplicabilidad y pertinencia en organizaciones similares.

Metas por alcanzar por objetivo

Cuadro 1. Metas por alcanzar

Objetivo	**Meta**
Realizar un diagnóstico de la situación actual de la gestión de riesgos en el área de TI de las organizaciones financieras locales, mediante una evaluación que permita establecer una línea base para proponer mejoras concretas.	Informe detallado sobre el estado actual de la gestión de riesgos correspondiente al área de TI.
Examinar las mejores prácticas en el campo de las tecnologías de la información para la gestión de riesgos en TI, mediante una revisión documental de marcos normativos, estudios de caso y literatura, con el fin de contar con un referente técnico que permita orientar la mejora de la gestión de riesgos en las organizaciones financieras de carácter local.	Sistematización de buenas prácticas aplicadas a la gestión de riesgos tecnológicos.
Analizar las brechas entre la situación actual de la gestión de riesgos de las organizaciones financieras de carácter local y las mejores prácticas identificadas, mediante una comparación estructurada entre los hallazgos del diagnóstico y los referentes teóricos y normativos, con el fin de identificar áreas de mejora prioritarias y sustentar las propuestas de intervención.	Análisis de brechas de la situación actual y las mejores prácticas en la gestión de riesgos en TI mediante la técnica Hexámetro de Quintiliano.
Construir un manual de buenas prácticas para la gestión de riesgos de TI, con base en las brechas detectadas, las mejores prácticas estudiadas y las directrices emitidas por la SUGEF en Costa Rica, con el fin de proporcionar una herramienta práctica que fortalezca la gestión de riesgos en organizaciones financieras de carácter local.	Manual alineado con las directrices de la SUGEF y basado en las mejores prácticas para la gestión de riesgos en Tecnologías de la Información.
Validar el manual de buenas prácticas elaborado, mediante el criterio de expertos del área de TI y gestión de riesgos en el sector financiero, para determinar su impacto potencial, aplicabilidad y pertinencia en organizaciones similares.	Validación y confiabilidad del manual ante los tomadores de decisiones y usuarios finales.

Fuente: Elaboración propia.

CAPÍTULO 2. MARCO TEÓRICO O CONCEPTUAL

Este capítulo presenta la base teórica que sustenta el presente trabajo final de graduación, abordando los principios y enfoques relacionados con la gestión de riesgos en Tecnologías de la Información (TI) en instituciones financieras de carácter local en Costa Rica. Estas instituciones operan principalmente dentro del territorio nacional y ofrecen servicios financieros a personas, empresas y sectores productivos del país.

Comprender la gestión de riesgos en TI resulta fundamental para identificar amenazas, mitigar impactos y garantizar tanto la continuidad operativa como el cumplimiento regulatorio. En las secciones siguientes se presentan los conceptos fundamentales que sustentan este estudio.

Riesgo

Según ISO (2018, p. 1), el riesgo se define como “el efecto de la incertidumbre sobre los objetivos”. Ivanova (2021, p. 56) complementa esta definición al señalar que, en general, “los riesgos se distinguen en tecnológicos, de mercado, financieros, económicos, públicos, ambientales, políticos y de reputación; así como riesgos relacionados con la cooperación entre socios, la propiedad intelectual, los clientes, el personal, el conocimiento y la gestión”. Mientras que la SUGEF (2024, p. 21), indica que “las entidades financieras pueden enfrentar riesgo de crédito, riesgo de precio, riesgo de tasas de interés, riesgo de tipo de cambio, riesgo de liquidez, riesgo operativo, riesgo de tecnologías de información, riesgo legal, riesgo de reputación, riesgo de legitimación de capitales y riesgo de conglomerado”. Los riesgos en TI afectan de manera significativa el desempeño y la sostenibilidad de las instituciones, en gran medida debido a la dependencia crítica en las tecnologías de la información.

Riesgo en TI

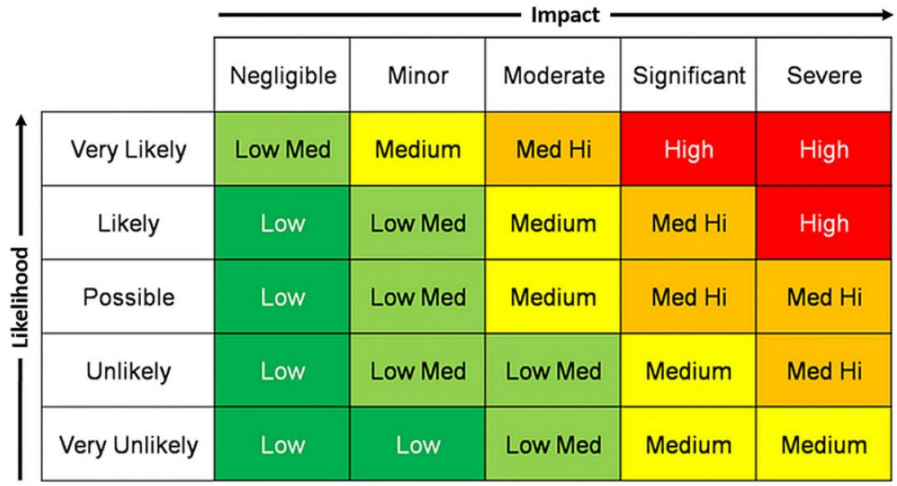
Según FSRA (2024, p. 6), “el riesgo de TI incluye pérdidas financieras, interrupción o daño operativo, o pérdida de reputación resultante de la insuficiencia, interrupción, destrucción, falla o daño por cualquier medio a los sistemas, infraestructura y datos de TI”. Lo anterior evidencia la importancia de abordar y mitigar los riesgos tecnológicos, no solo en términos de fallos técnicos, sino también considerando sus impactos financieros y estratégicos. Los riesgos en TI requieren una adecuada gestión, ya que esta resulta esencial para asegurar la estabilidad operativa y mantener la confianza de los clientes.

Gestión de riesgos en TI

Según ISO (2018, p. 1), la gestión de riesgos constituye “actividades coordinadas para dirigir y controlar la organización con relación a los riesgos”. Para la gestión de riesgos, es fundamental disponer de herramientas que posibiliten la evaluación y priorización de los

riesgos identificados en un proyecto, proceso u organización. Según Acebes et al. (2024, p. 1), “las matrices de riesgo son herramientas ampliamente reconocidas por académicos y profesionales en diversos sectores para evaluar y clasificar los riesgos según su probabilidad de ocurrencia y su impacto en los objetivos del proyecto”. Como se muestra en la Figura 1, la matriz de probabilidad e impacto es un instrumento del análisis cualitativo de riesgos que permite identificar, visualizar y jerarquizar los riesgos, facilitando la toma de decisiones sobre cómo distribuir los recursos para su control (Acebes et al., 2024).

Figura 1. Matriz de probabilidad e impacto



Fuente: Acebes et al. (2024, p. 4).

Principales líneas de defensa en la gestión de riesgos

La gestión de riesgos involucra líneas de defensa, las cuales permiten distribuir responsabilidades. Como primera línea, la dirección o responsables de los procesos operativos son los encargados de administrar el riesgo que surge en las actividades diarias. Sus funciones incluyen diseñar, poner en marcha y operar los controles pertinentes. La función de la segunda línea es proporcionar soporte y supervisión a la primera línea mediante el desarrollo e implementación de políticas, marcos y herramientas específicas diseñadas para la gestión de riesgos y el cumplimiento normativo. Finalmente, la tercera línea se encarga de ofrecer una garantía objetiva a la organización al evaluar la eficacia operativa de las otras líneas (Deloitte, 2020).

Marcos de gestión de riesgos

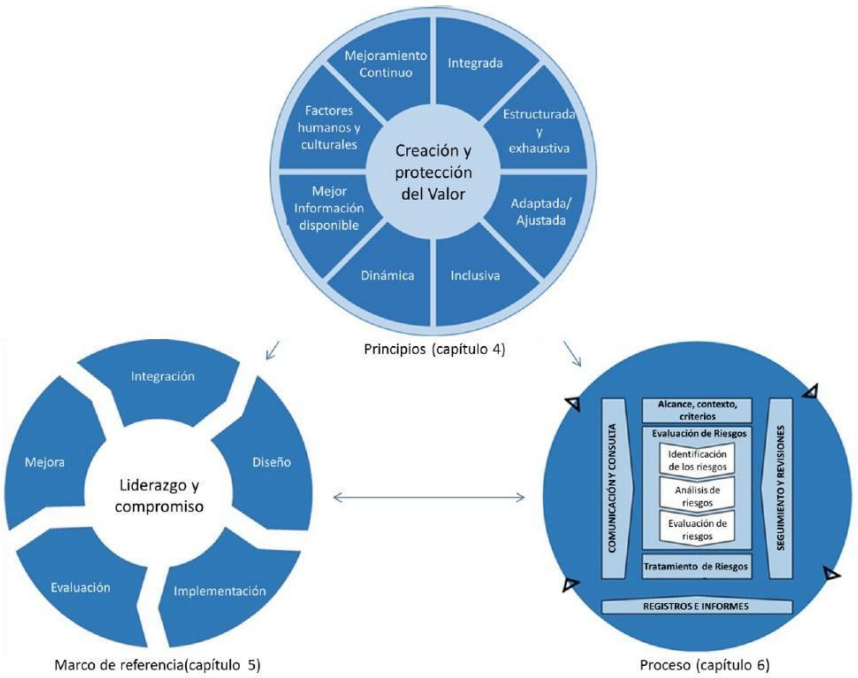
Con el objetivo de asegurar una gestión eficiente de riesgos, es importante que las organizaciones adopten marcos normativos que establecen una estructura metodológica sólida, sustentada en principios y prácticas reconocidas internacionalmente. Estos marcos facilitan la implementación sistemática y coherente de los procesos de identificación, análisis, tratamiento y monitoreo continuo de las amenazas que puedan comprometer el logro de los objetivos estratégicos.

Norma ISO 31000

La ISO 31000 define los principios básicos y las directrices para la gestión de riesgos a los que se enfrentan las organizaciones en diferentes momentos de su desarrollo. Según Ivanova (2021, p. 58), “la norma permite su uso tanto en el sector público como en el privado, independientemente de la naturaleza del riesgo y sus consecuencias (positivas o negativas), para proporcionar una metodología y reglas comunes para la gestión de riesgos”. La flexibilidad de esta norma le permite adaptarse a diversos contextos organizacionales, independientemente del tamaño o tipo de entidad, lo que la convierte en una herramienta estratégica para fortalecer la toma de decisiones.

En la figura 2, se muestran los componentes que conforman la norma. Según la ISO (2018) estos componentes pueden existir en la organización, pero podrían requerir ajustes para que la gestión de riesgos sea efectiva y coherente. Además, son esenciales porque proporcionan una estructura clara y sistemática para gestionar los riesgos de manera efectiva en cualquier organización.

Figura 2. Principios, marco de referencia y procesos.



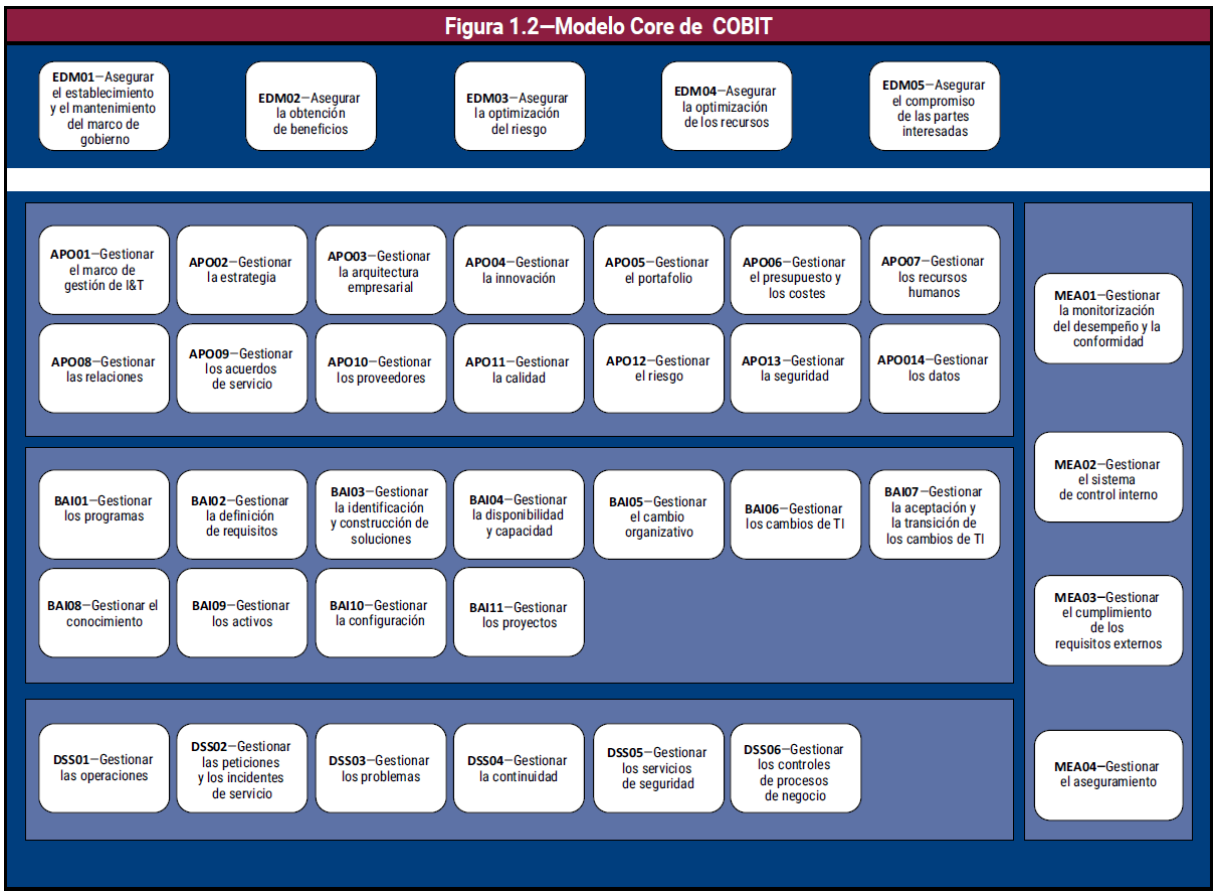
Fuente: ISO (2018, p. 6)

COBIT 2019

Además de la norma ISO 31000, COBIT 2019 constituye un marco de referencia complementario para el gobierno de la información, la gestión tecnológica y el control organizacional. Según (ISACA, 2018), este marco define la estrategia general y las directrices de buenas prácticas, que luego la organización adapta a sus procesos, políticas y procedimientos específicos.

De acuerdo con ISACA (2018), se organiza en objetivos de gobierno y gestión que forman el marco de referencia para la administración de la información y la tecnología (ver Figura 3).

Figura 3. Modelo Core de COBIT



Fuente: ISACA (2018, p. 12).

Los objetivos de gobierno, agrupados en el dominio Evaluar, Dirigir y Monitorizar (EDM), establecen que “el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia” (ISACA, 2018, p. 11).

Por su parte, los objetivos de gestión se organizan en cuatro dominios principales:

- Alinear, Planificar y Organizar (APO): aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología (I&T).
- Construir, Adquirir e Implementar (BAI): se encarga de la definición, adquisición e implementación de soluciones y su integración en los procesos de negocio.
- Entregar, Dar Servicio y Soporte (DSS): aborda la entrega operativa y el soporte de los servicios de información y tecnología, incluida la seguridad.

- Monitorizar, Evaluar y Valorar (MEA): aborda la monitorización del rendimiento y la conformidad de I&T con los objetivos de rendimiento internos, los objetivos de control interno y los requisitos externos.

El marco COBIT identifica siete componentes esenciales que sustentan el sistema de gobierno de la información y la tecnología, tales como los procesos, las estructuras organizativas, los principios, políticas y procedimientos, la información, la cultura, ética y comportamiento, las personas, habilidades y competencias, y los servicios, infraestructura y aplicaciones.

Para esta investigación, se consideran las prácticas de gestión de COBIT 2019 relacionadas con los objetivos de APO (Alinear, Planificar y Organizar) y MEA (Monitorear, Evaluar y Valorar) pertenecientes al componente “Procesos”. Se seleccionan por su relevancia tanto en la gestión del personal de TI como en la administración efectivo del riesgo. Seguidamente, se muestra la lista de prácticas consideradas.

- APO07.02 - Identificar al personal clave de TI
- APO07.03 - Mantener las habilidades y competencias del personal:
- APO07.04 - Evaluar y reconocer el rendimiento del personal:
- APO12.01 - Recopilar datos
- APO12.03 - Mantener un perfil de riesgo
- APO12.04 - Articular el riesgo
- MEA01.01 - Establecer un enfoque de supervisión

Técnica de Evaluación y Revisión de Programas (PERT)

Para la implementación, y en particular para estimar la duración de cada actividad incluida en este manual, se utilizará el método PERT. De acuerdo con Bagshaw (2021, p. 219), esta técnica realiza “tres estimaciones de tiempo para cada actividad, asumiendo una distribución de probabilidad beta para dichas estimaciones. El tiempo esperado para cada actividad puede aproximarse mediante el siguiente promedio ponderado”. Estas estimaciones se designan como:

a = estimación de tiempo optimista, es decir, el tiempo mínimo razonable necesario para realizar una actividad.

b = estimación de tiempo pesimista, es decir, el tiempo máximo razonable necesario para realizar una actividad.

m = estimación de tiempo más probable, es decir, el tiempo más probable aceptado para realizar una actividad.

El tiempo esperado (Te) que se aproxima a la media, la desviación estándar para la distribución beta se calcula de la siguiente forma:

$$T_e = \frac{a + 4m + b}{6}$$

Esta técnica permite reflejar de manera más realista la incertidumbre asociada a actividades con duraciones indeterminadas.

Regulaciones emitidas por la SUGEF

En Costa Rica, la SUGEF (s.f.) supervisa y regula a las entidades del sistema financiero, velando por su estabilidad y solidez. Esta función se lleva a cabo mediante normativas que solicitan el uso de marcos de gestión para estructurar procesos como la gestión de riesgos en TI, el control interno y el cumplimiento. A continuación, se presenta un resumen de las principales normativas relevantes para el estudio.

CONASSIF 5-24

Según el Consejo Nacional de Supervisión del Sistema Financiero (2024), este reglamento establece cómo las entidades financieras deben gestionar la gobernanza y los riesgos de la tecnología de información. Con respecto a los estándares internacionales, buenas prácticas y marcos de referencia mencionados, el Consejo Nacional de Supervisión del Sistema Financiero (2024, p. 7) señala que:

> “El marco de referencia COBIT 2019, emitido por ISACA, permite la alineación, interoperabilidad e integración con los estándares, buenas prácticas y otros marcos de referencia desarrollados por la industria y los profesionales de TI, lo cual fortalece el control interno de las tecnologías de información”.

Por lo tanto, el desarrollo de la solución propuesta en este estudio se fundamenta en este marco de gestión.

SUGEF 2-10

Según SUGEF (2024), cada entidad supervisada debe implementar un proceso formal y continuo de gestión de riesgos, acorde con la naturaleza, complejidad y tamaño de sus operaciones, así como con su perfil de riesgo. A continuación, se presentan los principales lineamientos en los que se fundamenta este estudio.

- Se debe garantizar que existan mecanismos de comunicación hacia lo interno de la entidad financiera de los alcances y resultados del proceso de Administración Integral de Riesgos, así como para determinar que su aplicación es efectiva (SUGEF, 2024, Art. 8).
- Se debe garantizar que se cuente con personal con los conocimientos y habilidades necesarios para desempeñar sus funciones dentro del proceso de administración de riesgos (SUGEF, 2024, Art. 8).
- Se debe considerar las responsabilidades y deberes de funcionarios involucrados en el proceso de Administración Integral de Riesgos (SUGEF, 2024, Art. 11).
- Se debe considerar verificar la recopilación y procesamiento de la información utilizada para la administración de los riesgos (SUGEF, 2024, Art. 17).

CAPÍTULO 3. MARCO METODOLÓGICO

En este capítulo se detalla la metodología de investigación empleada en el estudio. Se abordan aspectos como el enfoque y diseño de la investigación, la metodología utilizada, la población y la muestra, así como los instrumentos y técnicas de recolección de datos.

Enfoque de investigación

El presente estudio utiliza un enfoque cualitativo, cuyo propósito es comprender en profundidad las percepciones, experiencias y desafíos de los colaboradores involucrados en la gestión de riesgos en tecnologías de la información (TI), con el fin de desarrollar un conjunto de buenas prácticas fundamentadas en la realidad observada dentro de las organizaciones financieras de carácter local. Este enfoque permite identificar estrategias, limitaciones y aprendizajes que emergen de la experiencia cotidiana en la gestión de riesgos tecnológicos.

Análisis cualitativo

Según Hernández-Sampieri y Mendoza Torres (2018), “las investigaciones cualitativas suelen producir preguntas antes, durante y después de la recolección y análisis de datos”, lo cual permite adaptar el estudio conforme se obtiene nueva información relevante. En este caso, el análisis de la información obtenida mediante encuestas y entrevistas, permitirá identificar relaciones significativas entre las prácticas actuales de gestión de riesgos y los desafíos enfrentados por las organizaciones. Este proceso será fundamental para la elaboración del manual de buenas prácticas, ya que garantizará que las recomendaciones propuestas estén fundamentadas en evidencia empírica y contextualizada.

Tipo de investigación

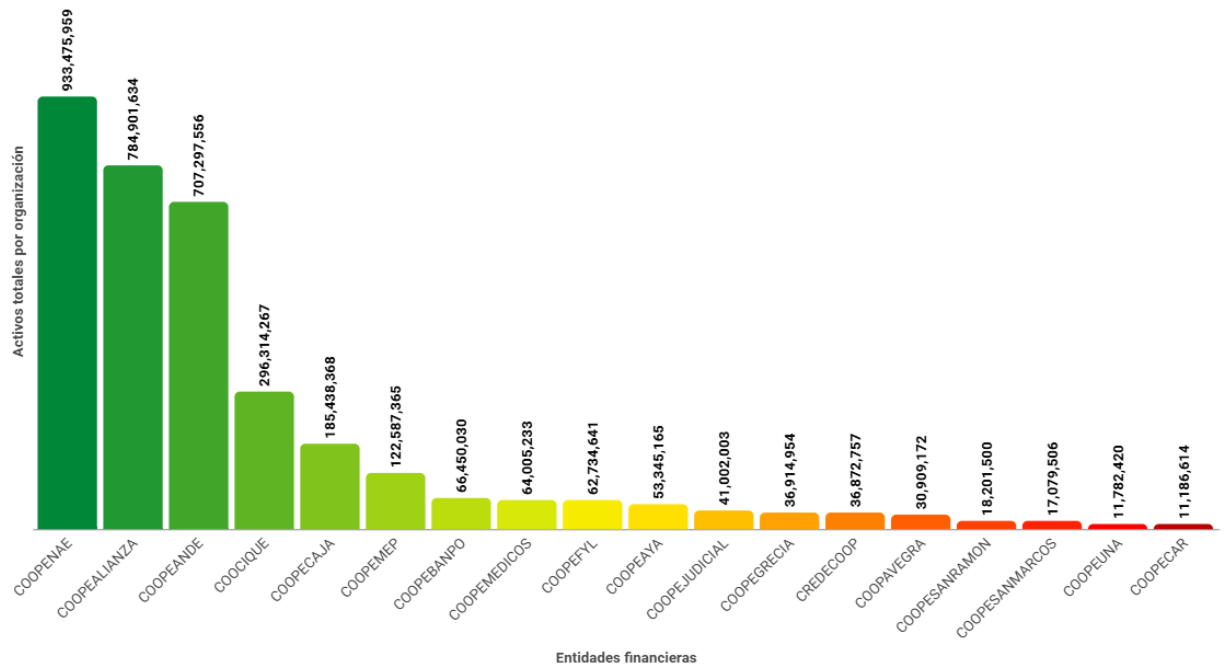
Esta investigación es de tipo aplicada, ya que tiene como propósito desarrollar un manual de buenas prácticas orientado a fortalecer la gestión de riesgos en tecnologías de la información en organizaciones financieras de carácter local. Para ello, se parte del análisis de la situación actual y del uso de marcos normativos reconocidos, con el fin de generar una propuesta útil, viable y contextualizada a las necesidades del sector.

Población y muestra

La población de esta investigación está conformada por colaboradores de organizaciones financieras de carácter local en Costa Rica que participan directamente en los procesos de gestión de riesgos en Tecnologías de la Información (TI). Se identificó que las cooperativas de ahorro y crédito presentan un nivel de activos bajo en comparación con otras

organizaciones financieras. Según la lista más reciente publicada en julio por la SUGEF (2025), un total de 18 cooperativas de ahorro y crédito se encuentran bajo su supervisión. En el Gráfico 1 se presentan las cooperativas de mayor tamaño según sus activos totales al corte de marzo de 2025, destacando seis que registran activos superiores a los cien mil millones de colones. Para este estudio se tomarán en cuenta las cooperativas cuyos activos totales se encuentren por debajo de dicho umbral.

Gráfico 1. Activos totales de cooperativas de ahorro y crédito supervisadas por la SUGEF al corte de marzo del 2025



Fuente: Elaboración propia.

Entre los perfiles considerados se incluyen gerentes de TI, encargados de seguridad de la información, oficiales de cumplimiento, auditores internos y otros profesionales con funciones relacionadas con la gestión tecnológica y el control de riesgos.

Para asegurar la pertinencia y profundidad de la información recolectada, se utilizará un muestreo no probabilístico por criterio, seleccionando intencionadamente a 8 colaboradores de organizaciones financieras locales que posean experiencia en la gestión de riesgos en Tecnologías de la Información. Esta estrategia permitirá obtener información relevante de acuerdo con los objetivos de estudio.

A continuación, se expone el cuadro correspondiente a la técnica empleada, la muestra seleccionada y el objeto de estudio.

Cuadro 2. Resumen del método de investigación

Técnica de recolección de datos	Tamaño muestral	Objeto de estudio	Producto esperado
Encuesta	8	Experiencias, desafíos y sugerencias sobre la gestión de riesgos en TI.	Diagnóstico preliminar de la situación actual de la gestión de riesgos en TI con base en percepciones y actitudes, utilizando análisis estadístico descriptivo (con escala de Likert)
Entrevista	3	Validación de hallazgos de encuestas, exploración en profundidad de prácticas y percepciones.	Análisis cualitativo que complemente y contraste los resultados de las encuestas, enriqueciendo el diagnóstico con perspectivas detalladas.

Elaboración: Elaboración propia

Instrumentos y técnicas utilizadas para la recolección de datos

Según Medina Romero et al. (2023, p. 13), señala que “una técnica de investigación es un enfoque general para la recolección y el análisis de información, mientras que un instrumento de investigación es una herramienta específica utilizada dentro de una técnica de investigación para recopilar información”. En el marco de esta investigación, se hace uso de ambos términos.

Encuestas

Según Medina Romero et al. (2023, p. 23), “es una técnica de investigación que se utiliza para recopilar información de un gran número de personas”. También se indica que “se trata de una herramienta versátil y accesible que permite a los investigadores obtener información sobre comportamientos, actitudes, opiniones y demografía de una población objetivo”. Se

empleará la escala de Likert, una herramienta que permite medir actitudes, opiniones y percepciones sobre un tema específico. Las preguntas estarán orientadas a explorar las experiencias, desafíos y sugerencias de los participantes en relación con la gestión de riesgos en TI, lo cual permitirá que los hallazgos obtenidos reflejen la situación actual.

Entrevistas

“Involucra la interacción directa entre el entrevistador y el entrevistado con el objetivo de obtener información y opiniones detalladas sobre un tema específico” (Medina Romero et al., 2023, p. 26). Se llevarán a cabo entrevistas con el propósito de validar los hallazgos derivados de la aplicación de las encuestas. Por cada entrevista se realiza una minuta que documenta los puntos clave abordados, percepciones del entrevistado y observaciones relevantes, lo cual permitirá complementar el análisis y fortalecer el diagnóstico de la situación actual.

Hexámetro Quintiliano

El Hexámetro de Quintiliano “consiste en contestar a seis preguntas, el qué, quién, cuándo, por qué, dónde y cómo” (Callow Monge, 2021). A partir de los datos recopilados mediante encuestas, entrevistas y revisión de literatura, se aplica esta técnica con el objetivo de identificar áreas de mejora en la situación actual de la gestión de riesgos en TI en instituciones financieras de carácter local, con el fin de contribuir a la elaboración de un manual de buenas prácticas.

Revisión de literatura

La revisión de literatura “implica la revisión y evaluación sistemática de documentos escritos, tales como informes, transcripciones, registros y publicaciones, con el objetivo de obtener información y comprender mejor un fenómeno o un problema específico” (Medina Romero et al., 2023, p. 30).

Estrategia de búsqueda literaria

Se llevará a cabo una revisión de documentos relacionados con la gestión de riesgos en el área de Tecnologías de la Información (TI), utilizando diversas fuentes de información. Entre estas se incluyen bases de datos académicas como Business Source Ultimate y SIDUNA, así como sitios web oficiales de normativas, libros especializados y otras publicaciones relevantes. Además, se emplearán herramientas basadas en inteligencia artificial, como NotebookLM y Perplexity, para facilitar la búsqueda de artículos científicos, tesis y otros documentos pertinentes.

Cuadro 3. Revisión de literatura

Nombre	Tipo	Año	Autor(es)	Base de datos	Detalles
Norma Internacional 1SO 31000:2018	Norma	2018	International Organization for Standardization (ISO)	Página oficial de la ISO	Proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones.
COBIT 2019	Marco de referencia	2018	COBIT Working Group	Página oficial de ISACA	Proporciona un marco integral para el gobierno y la gestión de TI, ayudando a las organizaciones a alinear sus objetivos de negocio, gestionar el riesgo, optimizar los recursos y asegurar el cumplimiento normativo.
IT Risk and IT Audit Working Together to Reduce the Burden on the Business	Artículo	2023	Benjamin Bartz	ISACA Journal	Propone que la gestión de riesgos y la auditoría de TI colaboren para reducir la carga en el negocio, apoyándose en: cultura de apoyo, auditores con visión en “T”, pruebas efectivas de controles y uso de herramientas comunes.
Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach	Artículo	2020	H. M. Alshahrani S. S. Alotaibi M. T. J. Ansari M. M. Asiri A. Agrawal R. A. Khan H. Mohsen A. M. Hilal	Publicado en la revista Applied Sciences, obtenido de EBSCO	Propone usar Fuzzy TOPSIS para evaluar y priorizar riesgos en TI, manejando incertidumbre y subjetividad.

The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity	Artículo	2024	Stavros Kalogiannidis, Dimitrios Kalfas, Olympia Papaevangelou, Grigoris Giannarakis y Fotios Chatzitheodoridis	ResearchGate	Analiza cómo la inteligencia artificial (IA) mejora la evaluación predictiva de riesgos y la continuidad empresarial.
Propuesta de metodología para la gestión de riesgos de TI basada en las mejores prácticas internacionales para la empresa Information Evolution Costa Rica.	TFG	2024	Fabiana Herrera Madriz	Repositorio TEC	Busca transformar la gestión de riesgos de TI en la empresa de un enfoque reactivo a uno proactivo, alineado con los objetivos estratégicos y las mejores prácticas de la industria.

Fuente: Elaboración propia

Prompts clave

El diseño adecuado de instrucciones de búsqueda resulta fundamental para apoyar la obtención de información clave en la investigación. Seguidamente, se presenta un compendio de los principales prompts utilizados.

- Search for books or academic articles that address technology risk management from the year 2020 onwards.
- Search for articles on IT risk assessment from 2020.
- Find academic publications addressing IT governance and risk management since 2020.
- Locate publications that analyze risk management and prioritization in technological contexts from 2020 onwards.

CAPÍTULO 4. DIAGNÓSTICO Y ANÁLISIS DE RESULTADOS

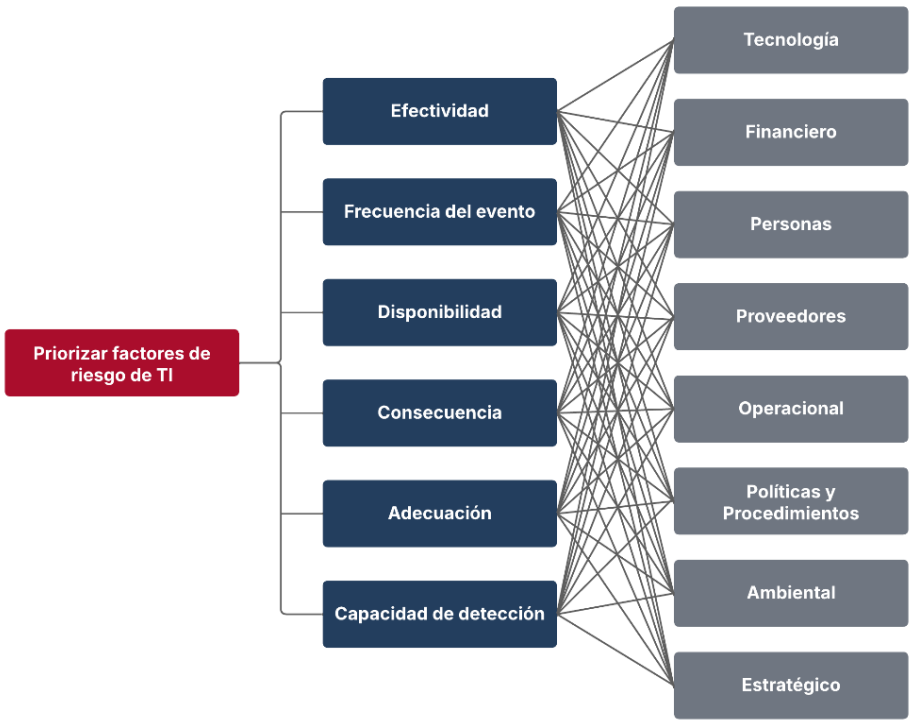
Resultados de la revisión de literatura

1. Análisis y clasificación de factores de riesgo de TI utilizando el enfoque basado en TOPSIS difuso.

El objetivo principal del artículo es evaluar y jerarquizar los factores de riesgo en el ámbito de las Tecnologías de la Información, identificando aquellos que deben ser abordados con mayor urgencia. Para ello, se emplea una técnica de toma de decisiones multicriterio (MCDM) basada en el enfoque difuso, utilizando específicamente el método TOPSIS (Técnica para el Ordenamiento de Preferencias por Similaridad con la Solución Ideal).

En relación con la jerarquía de la evaluación de factores de riesgos en TI, según Alshahrani et al. (2022), se han identificado ocho factores: Tecnología, Financiero, Personas, Proveedores, Operativo, Política y Procedimientos, Ambiental y Estratégico, que se denotan por A1, A2, A3, A4, A5, A6, A7 y A8, respectivamente. Para priorizarlos reconocieron algunos criterios, como la efectividad, la frecuencia de eventos, la disponibilidad, la consecuencia, la adecuación y la capacidad de detección, denotados por C1, C2, C3, C4, C5 y C6, respectivamente. La Figura 4 muestra la estructura jerárquica utilizada para evaluar los factores de riesgo en Tecnologías de la Información, mediante un enfoque difuso basado en TOPSIS.

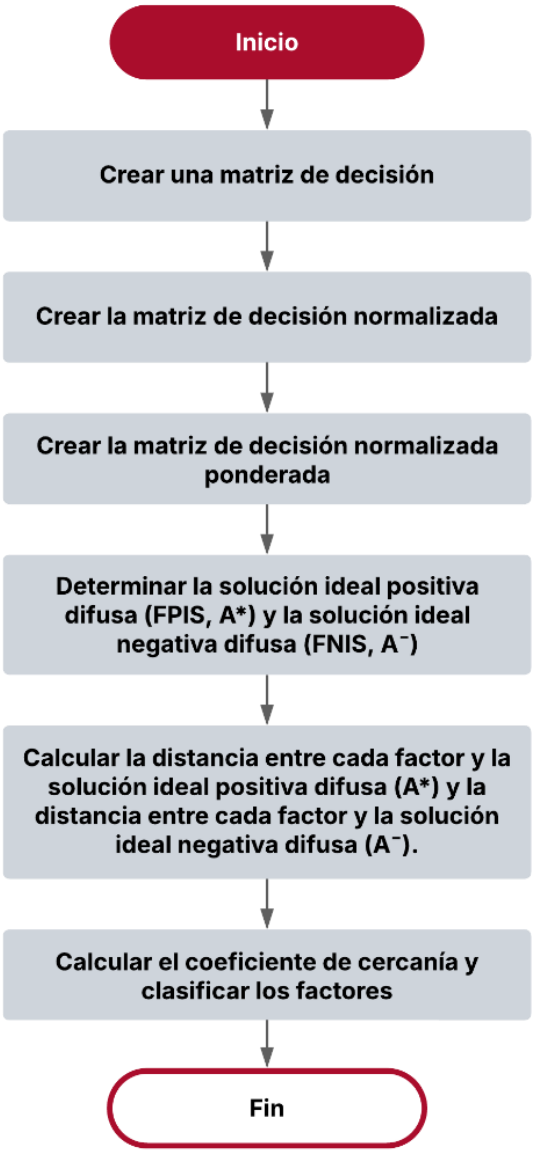
Figura 4. Estructura jerárquica para la evaluación



Fuente: Adaptado de Alshahrani et al. (2022, p. 6)

La técnica TOPSIS difusa es un enfoque desarrollado a partir del principio fundamental de TOPSIS para abordar una amplia variedad de desafíos de toma de decisiones multicriterio (MCDM) en un entorno de incertidumbre (Alshahrani et al.2022). La diferencia principal entre TOPSIS y TOPSIS difuso está en cómo utilizan los datos. TOPSIS usa números exactos para las valoraciones y los pesos. Por otro lado, TOPSIS difuso utiliza números difusos triangulares (TFNs), que permiten incorporar la incertidumbre e imprecisión inherentes a las decisiones humanas. En la Figura 5, se visualizan los pasos secuenciales del método TOPSIS difuso.

Figura 5. Pasos del método TOPSIS difuso.



Fuente: Adaptado de Alshahrani et al. (2022, p. 7)

El estudio concluye que la tecnología es el principal riesgo en las organizaciones, seguida de otros factores como el estratégico y financiero. Además, resalta la importancia de la seguridad informática, incluyendo amenazas internas. Según Alshahrani et al. (2022), este análisis de riesgos permitirá a la administración fundamentar adecuadamente las inversiones en el programa de gestión de riesgos, garantizando decisiones confiables.

2. El papel de la tecnología de inteligencia artificial en la evaluación predictiva de riesgos para la continuidad del negocio

Según Kalogiannidis et al. (2024), el objetivo de la investigación es “comprender cómo los diferentes componentes de IA, como el procesamiento del lenguaje natural (PLN), el análisis de datos impulsado por IA, el mantenimiento predictivo impulsado por IA y la integración de IA en la planificación de respuesta a incidentes, mejoran la evaluación de riesgos y respaldan la continuidad del negocio en un entorno donde las empresas enfrentan una miríada de riesgos, incluidos desastres naturales, ciberataques y fluctuaciones económicas. Se utilizó un diseño transversal y un método cuantitativo para recopilar datos para este estudio de una muestra de 360 especialistas en tecnología”. Los autores sugieren que las organizaciones deberían priorizar el desarrollo de capacidades relacionadas con la inteligencia artificial, haciendo especial énfasis en áreas como el procesamiento del lenguaje natural (PLN) para facilitar la evaluación automatizada de riesgos, el análisis de datos para una detección oportuna de amenazas, el mantenimiento predictivo como estrategia para optimizar operaciones.

3. El riesgo de TI y la auditoría de TI trabajando juntos para reducir la carga sobre el negocio

El artículo de Bartz (2023) propone una colaboración efectiva entre los equipos de auditoría informática y gestión de riesgos de TI para reducir la carga sobre las operaciones del negocio. Para que esta alianza sea efectiva, se deben cumplir cuatro principios fundamentales: fomentar una cultura de apoyo, contar con auditorías de TI con perfiles en forma de “T”, asegurar que el riesgo de TI evalúe correctamente la efectividad de los controles, y utilizar herramientas comunes.

La cultura organizacional juega un rol esencial. No se debe ver la seguridad como un simple requisito a cumplir, ni temer a la auditoría. En cambio, los empleados deben entender desde el inicio de su carrera la relevancia de estas funciones. “El riesgo ayuda al negocio a tomar decisiones informadas. La auditoría descubre brechas en los procesos organizacionales” (Bartz, 2023, p. 20). En cuanto a la necesidad de contar con equipos de auditoría en forma de

“T”, esto implica contar con profesionales que posean un conocimiento general amplio y habilidades técnicas profundas en áreas específicas, como señala Bartz (2023, p. 21), estos equipos “tienen una amplia base de conocimientos fundamentales en auditoría y conocimientos técnicos”.

Por su parte, el riesgo de TI debe ser capaz de probar la efectividad de los controles y documentarlo adecuadamente. Esto permite que la auditoría, que debe mantener su independencia, pueda apoyarse en estas pruebas sin duplicar esfuerzos. Según Bartz (2023), para garantizar la confiabilidad de su trabajo, el equipo de riesgos debe manejar tanto la información proporcionada por la entidad (IPE) como la utilizada por la empresa (IUC).

Para promover la colaboración entre equipos, los equipos de riesgo y auditoría deben alinear sus herramientas. “Usar una plataforma compartida para auditorías y evaluaciones de riesgo permite que ambos equipos aprovechen el trabajo de cada uno” (Bartz, 2023, p. 22).

Cuando los equipos de auditoría y riesgos están bien coordinados, pueden revisar la seguridad de la organización mejor, sin detener tanto el trabajo diario. Según Bartz (2023), la auditoría y la gestión de riesgos de TI cumplen funciones diferentes, pero ambas buscan proteger la organización.

4. Propuesta de metodología para la gestión de riesgos de TI basada en las mejores prácticas internacionales para la empresa Information Evolution Costa Rica.

La investigación propone una metodología de gestión de riesgos de TI para la empresa Information Evolution Costa Rica. Según Herrera Madriz (2024), a partir del análisis de los resultados, se determinó que la empresa no contaba con un proceso formal para la gestión de riesgos de TI, lo que generaba una gestión reactiva ante los incidentes. La metodología propuesta busca formalizar este proceso para asegurar la continuidad operativa y minimizar impactos adversos.

La metodología propuesta se sustenta en los marcos de referencia para la gestión de riesgos en TI. Según Herrera Madriz (2024), se llevó a cabo la investigación de la literatura sobre las mejores prácticas en gestión de riesgos de TI, identificando las prácticas recomendadas por COBIT 19, ISO 31000 y otras normativas relevantes. También se toman de referencia las metodologías OCTAVE, MARGERIT 3.0 e ISO/IEC 27005. En la figura 5, se muestran los pilares de la investigación.

Herrera Madriz definió tres fases para el proyecto, basándose en la identificación de buenas prácticas. La primera fase consiste en analizar la situación actual del proceso de gestión de riesgos de TI. La segunda fase se centra en la comparación y selección de las mejores prácticas en esta área. Finalmente, la tercera fase contempla la elaboración de los artefactos

necesarios para la implementación de la metodología de gestión de riesgos de TI. En el Cuadro 4 se detallan, por fase, las variables, los instrumentos aplicados y los sujetos involucrados en la investigación.

Cuadro 4. Operacionalización de las variables

Objetivo	Fase	Variable	Instrumentos	Sujetos de Investigación
OE 1	I	Situación actual de las prácticas de gestión de riesgos de TI.	- Revisión documental del proceso de gestión de riesgos (Apéndice E) - Entrevista semiestructurada (Apéndice C) - Notación BPMN	- Administrador de TI - Gerente general - Líder de operaciones
		Fortalezas y debilidades en las prácticas actuales.	- Revisión documental del proceso. (Apéndice E) - Entrevista semiestructurada (Apéndice C) - Análisis FODA (Apéndice I)	- Administrador de TI - Líder de operaciones
		Brechas de los procesos de gestión de riesgos.	- Revisión documental del proceso (Apéndice E) - Grupo focal (Apéndice F)	- Administrador de TI - Líder de operaciones
OE 2	II	Mejores prácticas en la gestión de riesgos de TI	- Revisión documental de las mejores prácticas de la industria - Análisis comparativo entre las mejores prácticas (Apéndice G)	Los instrumentos no se aplican a sujetos de información.
		Mejores prácticas de la industria seleccionadas	- Lista de verificación de las mejores prácticas y las necesidades de la empresa. (Apéndice H)	- Administrador de TI - Líder de operaciones
OE 3	III	Artefactos para la metodología	- Notación BPMN - Plantillas de los artefactos desarrollados - Revisión documental de las mejores prácticas	Los instrumentos no se aplican a sujetos de información.
		Metodología de Gestión de Riesgos de TI	- Revisión documental de las mejores prácticas - Hoja de ruta de implementación	Los instrumentos no se aplican a sujetos de información.
		Estandarización de la ejecución del proceso	- Lista de verificación para garantizar que todas las actividades estén cubiertas (Apéndice H) - Lista de verificación para el nivel de capacidad del proceso (Apéndice O)	- Administrador de TI - Líder de operaciones

Fuente: Herrera Madriz (2024)

Diagnóstico de la situación actual

El estudio se fundamenta en la aplicación de encuestas y entrevistas para recopilar información valiosa para este estudio. Se realizaron encuestas en línea a través de Microsoft Forms empleando la escala de Likert en la mayoría de ítems (ver Cuadro 5), así como entrevistas dirigidas a profesionales con experiencia en la gestión de riesgos en tecnologías de la información en instituciones financieras (ver Anexo 1 - 3).

Cuadro 5. Escalas de Likert empleadas en el instrumento de encuesta

Tipos de niveles			**Valor**
Muy bajo	Muy débil	Totalmente en desacuerdo	1
Bajo	Débil	En desacuerdo	2
Moderado	Moderada	Ni de acuerdo ni en desacuerdo	3
Alto	Fuerte	Acuerdo	4
Muy alto	Muy fuerte	Totalmente de acuerdo	5

Fuente: Elaboración propia

Se utilizó el coeficiente Alfa de Cronbach para medir la confiabilidad y consistencia interna de los ítems de la encuesta. La ecuación (ver Figura 6), "se calcula a partir de la varianza de los ítems individuales y de la varianza de la suma de los ítems de cada participante, cuando los ítems de una escala se encuentran correlacionados" (Toro, Peña-Sarmiento, Avendaño-Prieto, Mejía-Vélez, & Bernal-Torres, 2022, p.18).

Figura 6. Ecuación del coeficiente Alfa de Cronbach

$$\alpha = \frac{N}{N-1}\left(\sigma_x^2 - \sum_{i=1} N\, \sigma_{Yi}^2 \Big/ \sigma_x^2\right)$$

Fuente: Toro et al. (2022, p. 18)

Según Toro et al. (2022, p. 18), "el N representa el número de ítems de la escala, σ_x^2 la varianza de los puntajes observados, y σ_{Yi}^2 la varianza de los ítems i por cada persona". Además,

indican que valores con rangos <0.5 son inaceptables, >0.5 pobres, >0.6 cuestionable, >0.7 aceptable, >0.8 bueno, y >0.9 excelente (ver Cuadro 5).

Cuadro 6. Clasificación de la consistencia interna según el valor del Alfa de Cronbach

Alfa de Cronbach	**Consistencia interna**
α ≥ 0.9	Excelente
0.8 ≤ α < 0.9	Buena
0.7 ≤ α < 0.8	Aceptable
0.5 ≤ α < 0.6	Pobre
α ≤ 0.5	Inaceptable

Fuente: Uedufy (2023)

Para realizar el cálculo, primero se suman las puntuaciones obtenidas por cada colaborador y por cada ítem en las encuestas. Se detallan a continuación los elementos que componen la tabla (ver Cuadro 7):

- Columnas I1 a I5: representan los ítems evaluados en la encuesta, cada valor corresponde a la puntuación recibida de un colaborador en el ítem.
- Fila T1: representa la puntuación total por ítem, corresponde a la suma de las puntuaciones de todos los colaboradores en ese ítem.
- Columna T2: representa la puntuación total por colaborador, corresponde a la suma de sus puntuaciones de los ítems I1 al I5.
- Total: el último valor de la columna (T1) representa la suma de todas las puntuaciones de todos los colaboradores en todos los ítems.

A continuación, se describen los tres pasos a seguir:

Paso 1. Calcular la varianza de las puntuaciones totales de los colaboradores (σ_x^2)

Primero se calcula la media de las puntuaciones totales de los colaboradores ($\overline{X}$). Para obtener la media, se suman todas las puntuaciones totales (T1) y se dividen entre el número de colaboradores (X), esto da como resultado 18.5. Luego, se calcula la varianza de las puntuaciones totales de los colaboradores (σ_x^2) la cual da como resultado 7.5, la fórmula correspondiente es:

$$\boldsymbol{\sigma_x^2} = \frac{\sum(T1i - \bar{X})^2}{X}$$

Paso 2. Calcular la suma de las varianzas de los ítems ($\sum_{i=1}^{N} \sigma_{Yi}^2$)

Primero, se calcula la media de cada ítem. Luego, se determina la varianza de cada uno y se suman. El resultado es 2,6875, y la fórmula correspondiente es:

$$\boldsymbol{\sigma_{Yi}^2} = \frac{\sum(Ii - \bar{X})^2}{X}$$

Paso 3. Calcular el coeficiente Alfa de Cronbach (α)

Finalmente, se sustituyen los valores obtenidos en los pasos anteriores para calcular el resultado.

- N = 5
- σ_x^2=7.5
- $\sum_{i=1}^{N} \sigma_{Yi}^2$ = 2.6875

$$\boldsymbol{\alpha} = \frac{5}{5-1}\left(\frac{7.5 - 2.6875}{7.5}\right) = 0.8021$$

El valor calculado para el Alfa de Cronbach es 0.802. Según Toro et al. (2022), una puntuación mayor a .8 se considera buena. Esto significa que la escala tiene una consistencia interna alta, lo cual es un indicador de que los ítems miden de manera conjunta un mismo tema.

Cuadro 7. Resultados obtenidos de la encuesta para la aplicación del coeficiente Alfa de Cronbach

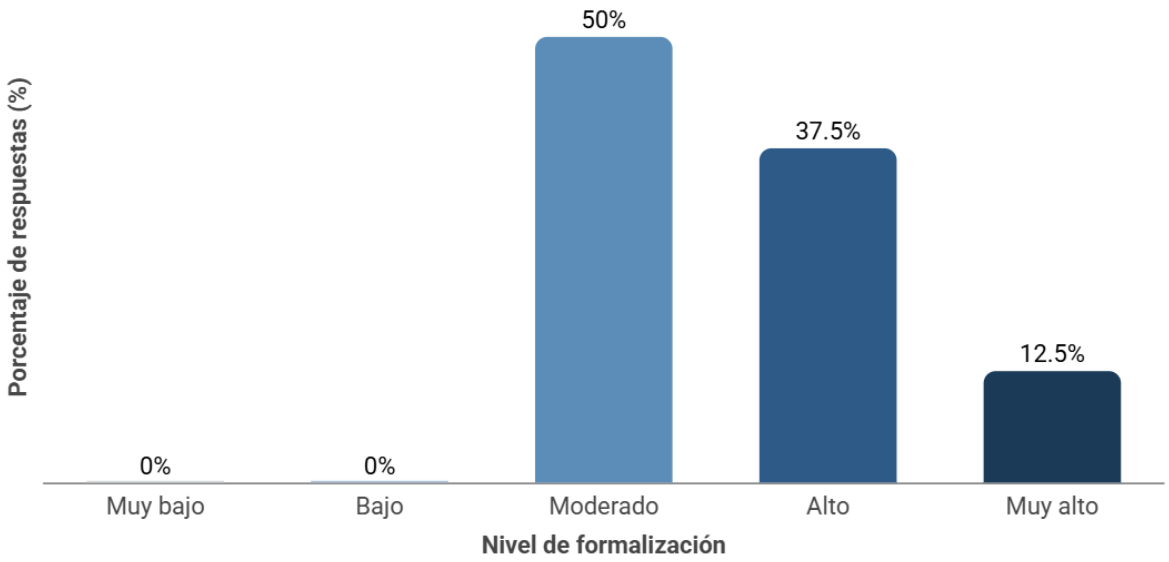
X	I1	I2	I3	I4	I5	T2
1	3	4	5	4	5	**21**
2	4	4	4	4	4	**20**
3	5	5	5	5	4	**24**
4	3	3	3	3	4	**16**
5	4	3	4	3	3	**17**
6	3	3	4	3	3	**16**
7	3	3	4	2	4	**16**
8	4	3	4	3	4	**18**
T1	**29**	**28**	**33**	**27**	**31**	**148**

Fuente: Elaboración propia a partir de los resultados de las encuestas aplicadas.

Preguntas aplicadas en la encuesta

1. ¿Cuál es el nivel actual de formalización de los procesos de gestión de riesgos de TI en su institución?

Gráfico 2. Nivel de formalización de los procesos de gestión de riesgos de TI

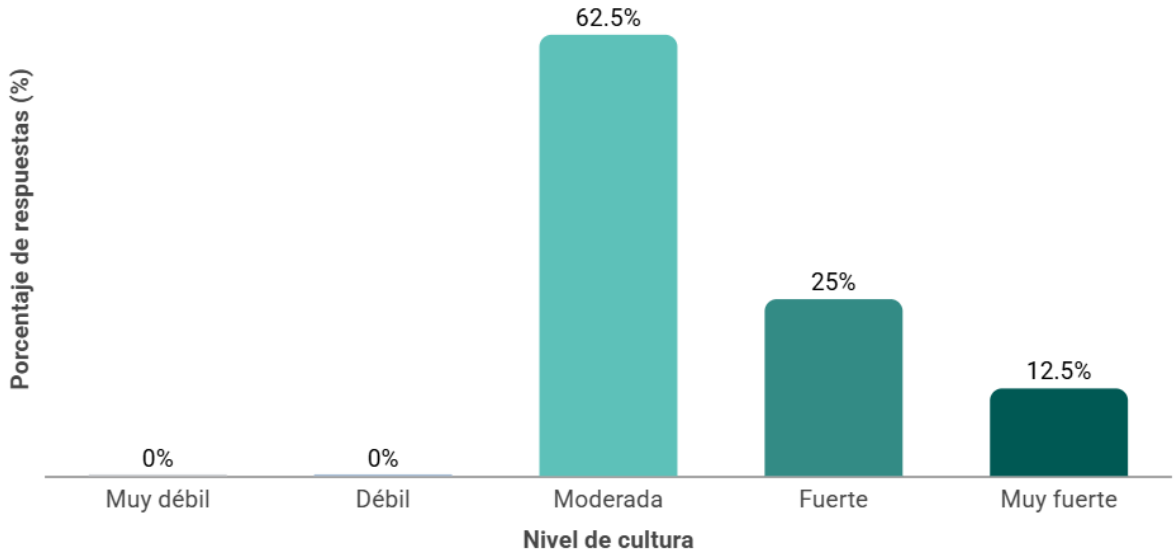


Fuente: Elaboración propia

En relación con el nivel de formalización de los procesos de gestión de riesgos en TI, el 50% de las instituciones encuestadas presenta un nivel moderado, mientras que el otro 50% alcanza niveles de alto a muy alto. Esto indica que, aunque todas las organizaciones han avanzado en la formalización de estos procesos, aún existe un margen considerable para que una parte significativa los lleve al más alto nivel.

2. ¿Cómo evaluaría la cultura de gestión de riesgos de TI dentro de su institución?

Gráfico 3. Evaluación de la cultura de gestión de riesgos de TI

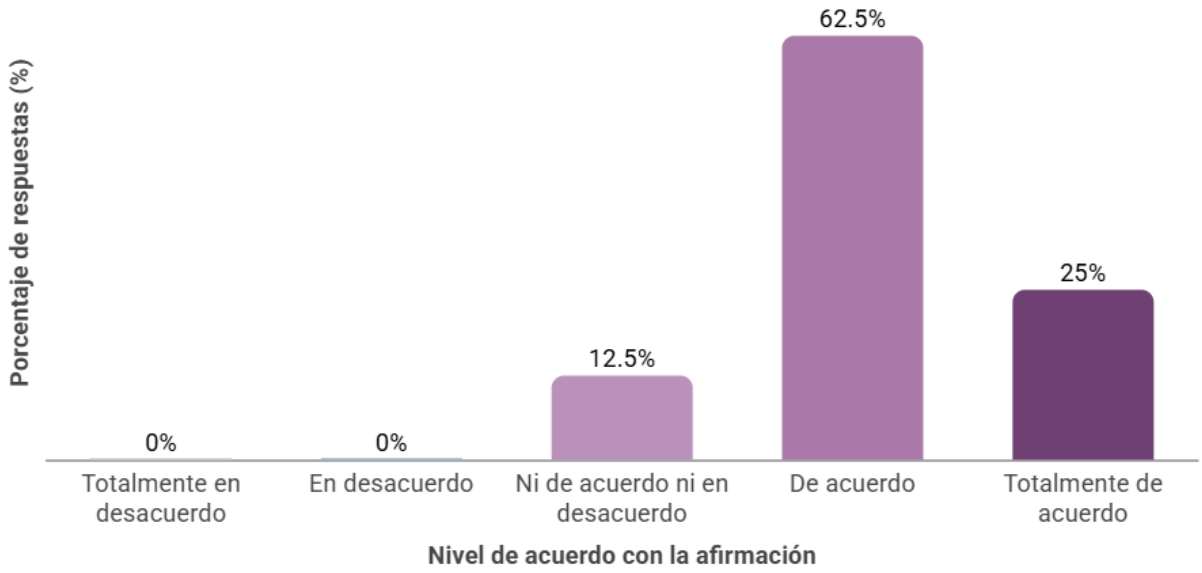


Fuente: Elaboración propia

El 62.5% de las instituciones evaluadas posee una cultura de gestión de riesgos de TI de nivel moderado. Un 25% la percibe como fuerte, mientras que el 12.5% la califica como muy fuerte. Esto evidencia que la cultura de gestión de riesgos presenta oportunidades de mejora en la mayoría de las organizaciones, lo que hace imprescindible su fortalecimiento para garantizar una gestión de riesgos efectiva.

3. Indique su nivel de acuerdo con la siguiente afirmación: "En mi institución, la identificación de riesgos en TI se realiza de forma estructurada, con procedimientos formalizados y metodologías definidas."

Gráfico 4. Evaluación de la formalización en la identificación de riesgos tecnológicos

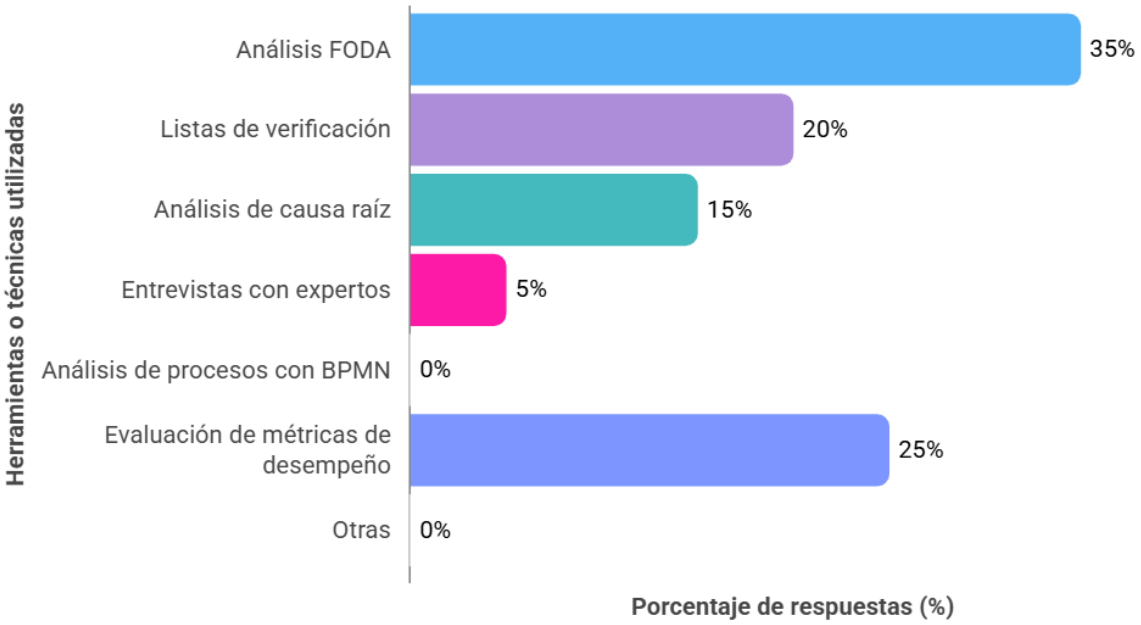


Fuente: Elaboración propia

La identificación estructurada de riesgos en TI es una práctica presente en la mayoría de las instituciones encuestadas, ya que el 62.5% está de acuerdo en que se realiza de manera estructurada. Además, un 25% se encuentra totalmente de acuerdo con esta afirmación, mientras que el 12.5% mantiene una posición neutral. Esto significa que la mayoría de las organizaciones disponen de procedimientos y metodologías claras para identificar los riesgos en TI.

4. ¿Qué herramientas o técnicas utiliza su organización en el proceso de identificación de riesgos en TI?

Gráfico 5. Herramientas y técnicas para la identificación de riesgos en TI

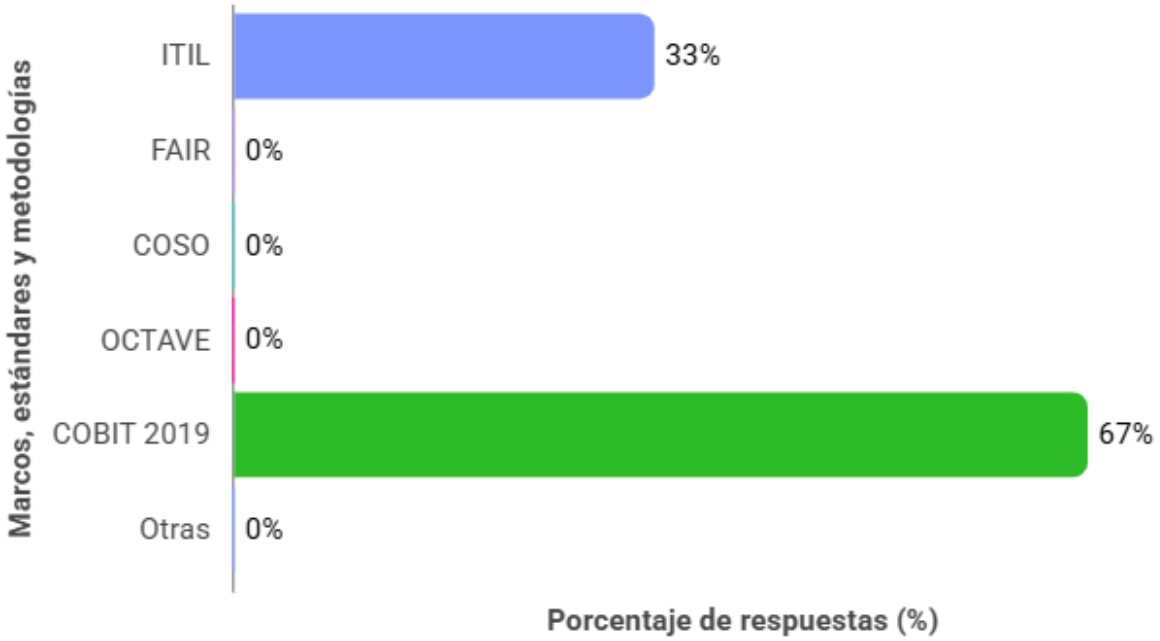


Fuente: Elaboración propia

Las herramientas más empleadas para identificar riesgos de TI son el análisis FODA con un 35% y la evaluación de métricas de desempeño con un 25%. Después se encuentran las listas de verificación con un 20%, el análisis de causa raíz con un 15% y, en menor medida, las entrevistas con expertos con un 5%. Estos resultados reflejan una inclinación hacia métodos de enfoque estratégico, destacando el análisis FODA como la herramienta más utilizada.

5. ¿Cuáles marcos, estándares o metodologías utilizan en su organización para la gestión de riesgos en TI?

Gráfico 6. Marcos, estándares y metodologías aplicados en la gestión de riesgos de TI

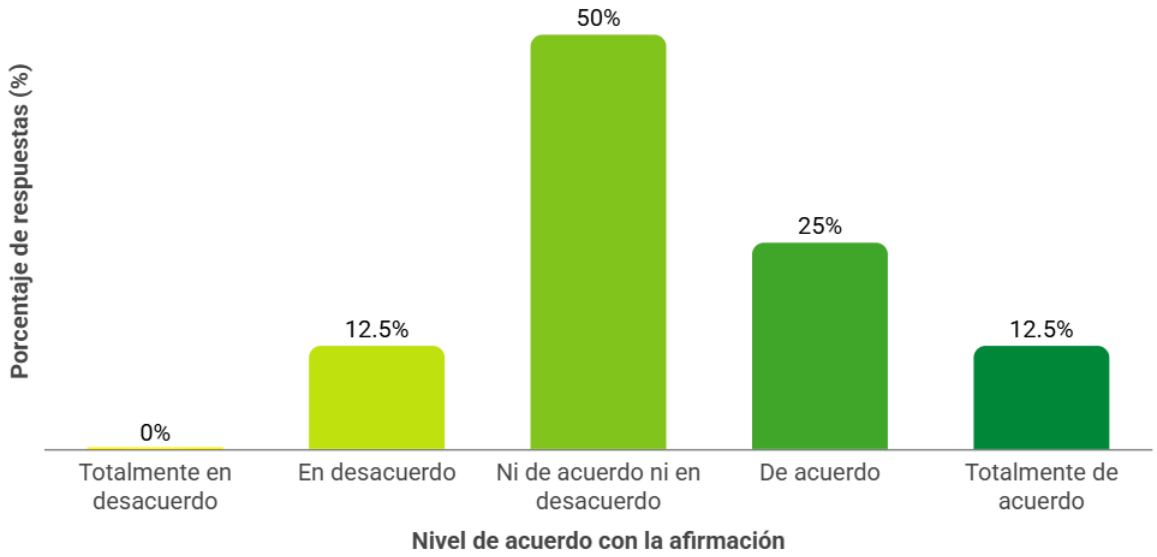


Fuente: Elaboración propia

El marco de referencia más empleado para la gestión de riesgos de TI es COBIT 2019, utilizado por el 67% de las organizaciones encuestadas, mientras que el 33% opta por ITIL. Estos resultados indican que COBIT 2019 se posiciona como la metodología principal, evidenciando un enfoque robusto en el gobierno y la gestión de TI.

6. Indique su nivel de acuerdo con la siguiente afirmación: "Considero que la colaboración entre la gestión de riesgos de TI y la auditoría interna en nuestra organización es efectiva y coordinada."

Gráfico 7. Evaluación de la colaboración entre la gestión de riesgos de TI y la auditoría interna

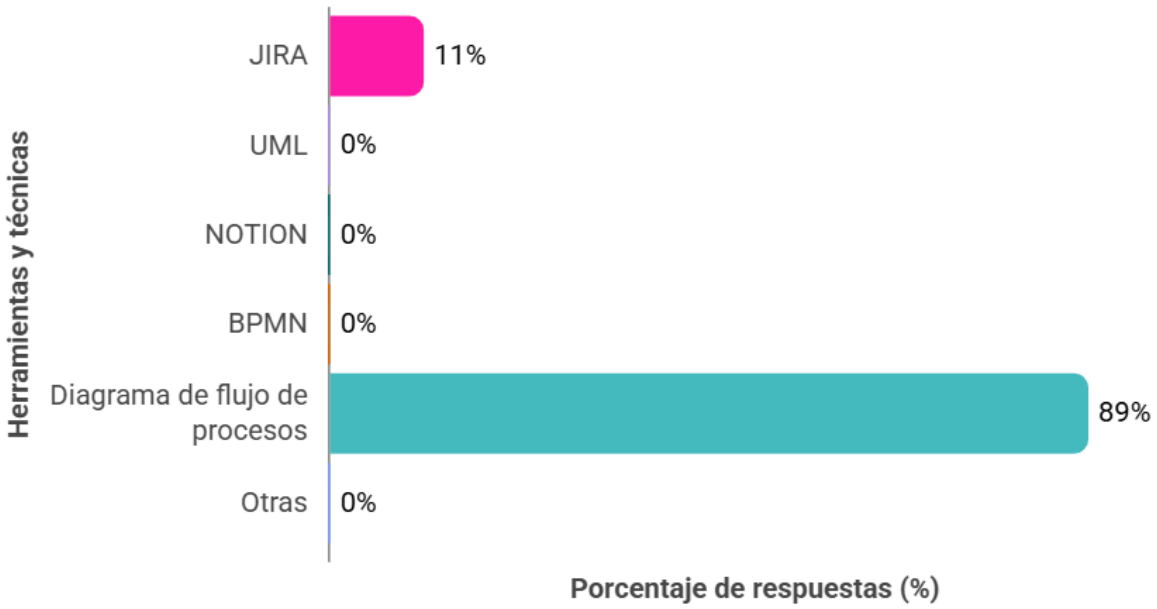


Fuente: Elaboración propia

Un 37.5% de los encuestados (25% de acuerdo y 12.5% totalmente de acuerdo) considera que existe una colaboración efectiva y coordinada entre la gestión de riesgos de TI y la auditoría interna. Sin embargo, el 50% mostró una postura neutral al respecto, y un 12.5% manifestó desacuerdo. Estos resultados muestran que en la mayoría de las organizaciones la colaboración entre gestión de riesgos de TI y auditoría interna no está completamente consolidada, lo que representa una oportunidad para fortalecer la comunicación y coordinación.

7. ¿Cuáles herramientas o técnicas utilizan es su organización para modelar y documentar los procesos de gestión de riesgos en TI?

Gráfico 8. Herramientas y técnicas para modelar y documentar los procesos de gestión de riesgos en TI

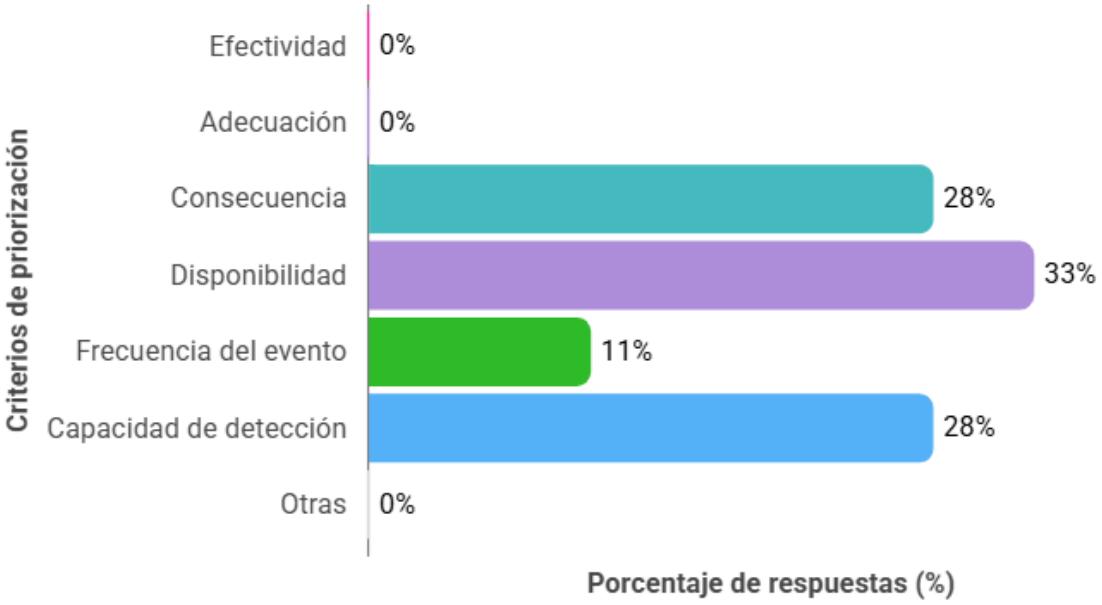


Fuente: Elaboración propia

El 89 % de las organizaciones utiliza diagramas de flujo de procesos para modelar y documentar la gestión de riesgos en TI, en contraste con el 11 % que emplea JIRA. Esto evidencia que los diagramas de flujo son la herramienta más empleada para representar y documentar estos procesos.

8. ¿Cuáles criterios utiliza su organización para priorizar los riesgos de TI?

Gráfico 9. Criterios para la priorización de riesgos de TI

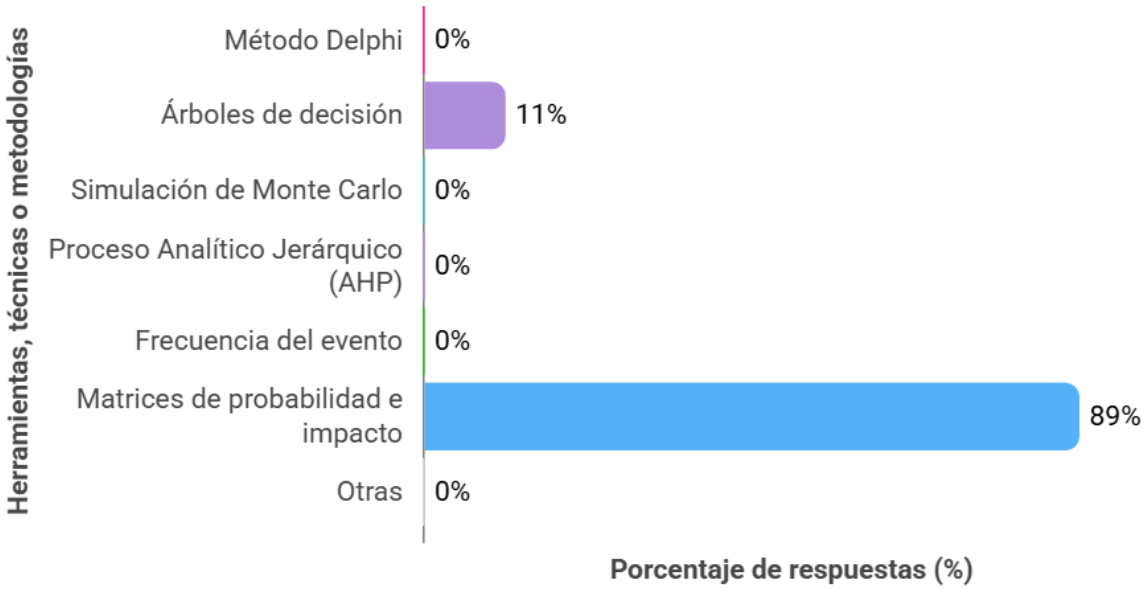


Fuente: Elaboración propia

Los criterios principales para priorizar los riesgos de TI son la disponibilidad con un 33 %, la consecuencia con un 28 % y la capacidad de detección también con un 28 %. Por otro lado, los criterios menos considerados son la frecuencia del evento con un 11 %, así como la efectividad y la adecuación de los controles, ambos con un 0 %.

9. ¿Cuáles herramientas, técnicas o metodologías utilizan es su organización para priorizar los riesgos en TI?

Gráfico 10. Herramientas, técnicas y metodologías para la priorización de riesgos en TI

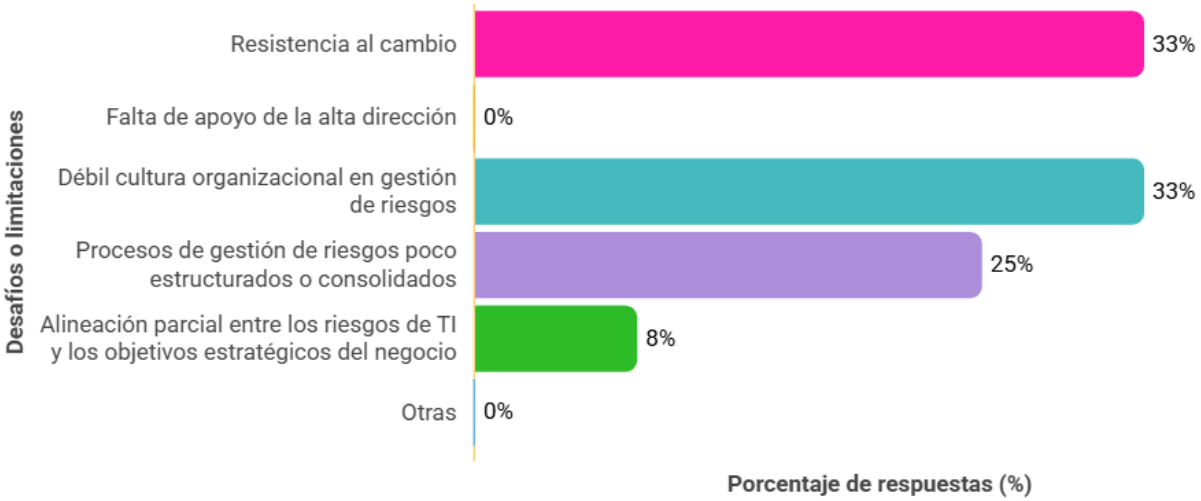


Fuente: Elaboración propia

El 89% de las organizaciones prioriza los riesgos en TI mediante matrices de probabilidad e impacto, mientras que el 11% recurre a árboles de decisión. Esto confirma que las matrices de probabilidad e impacto se han establecido como la herramienta estándar para la priorización de riesgos.

10. ¿Cuáles son los principales desafíos o limitaciones que enfrenta su institución al gestionar los riesgos de TI?

Gráfico 11. Principales desafíos y limitaciones en la gestión de riesgos de TI

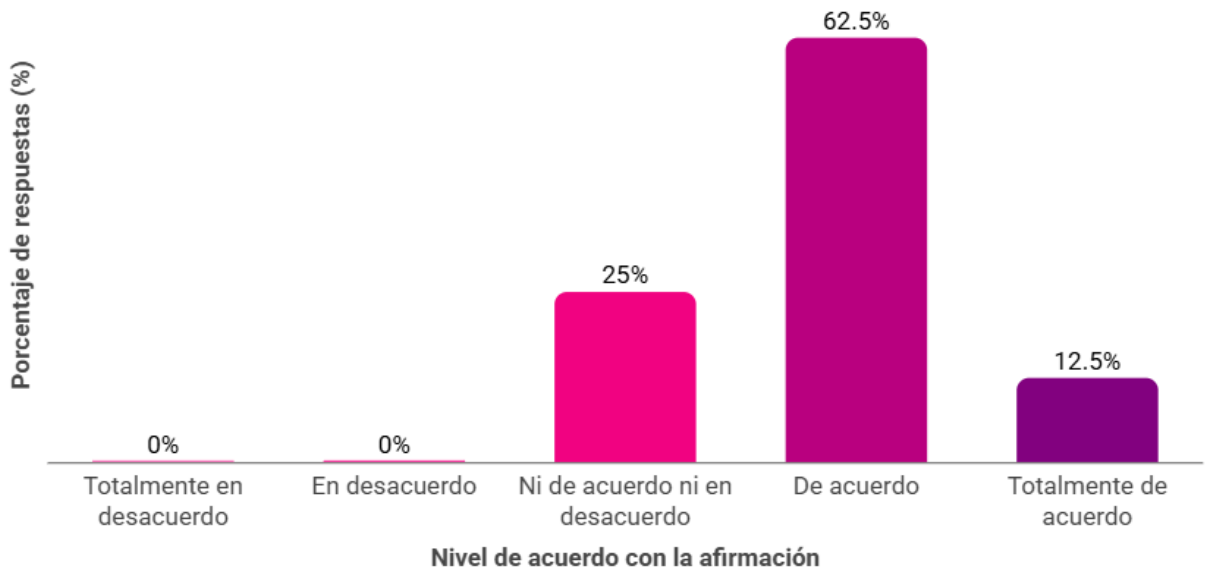


Fuente: Elaboración propia

Los principales desafíos en la gestión de riesgos de TI son la resistencia al cambio y una cultura organizacional débil en este ámbito, mencionados por el 33% de los encuestados. Además, un 25% señala como reto la falta de procesos de gestión de riesgos estructurados y consolidados, mientras que el 8% identifica la alineación parcial entre los riesgos de TI y los objetivos estratégicos del negocio. Estos resultados indican que los mayores obstáculos son principalmente culturales y organizacionales, más que técnicos.

11. Indique su nivel de acuerdo con la siguiente afirmación: "Mi organización integra activamente los riesgos tecnológicos emergentes (como la Inteligencia Artificial, computación en la nube, amenazas cibernéticas, entre otros) en sus prácticas de gestión de riesgos de TI."

Gráfico 12. Percepción sobre la integración de riesgos tecnológicos emergentes en la gestión de riesgos de TI

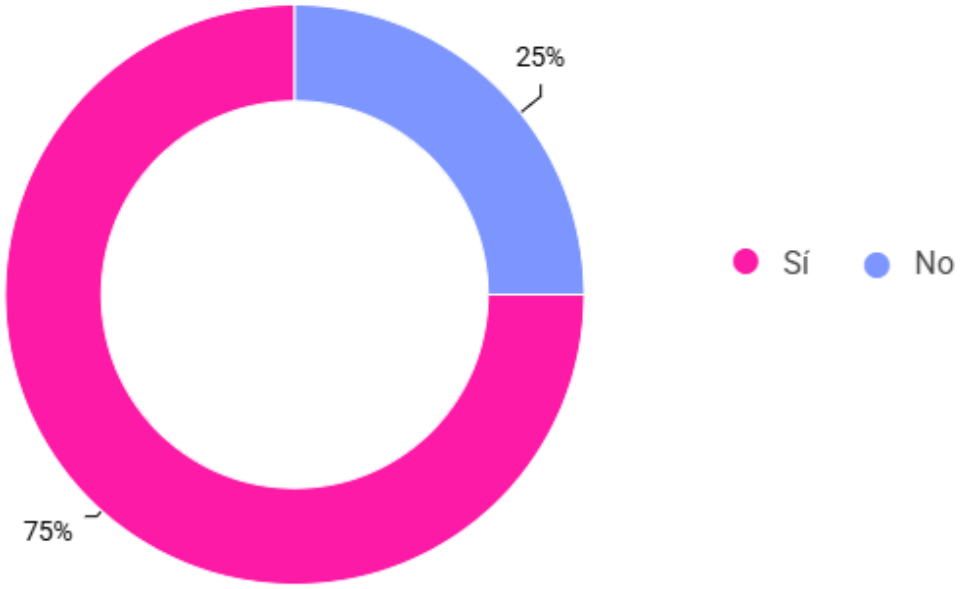


Fuente: Elaboración propia

La mayoría de las organizaciones encuestadas están gestionando activamente los riesgos tecnológicos emergentes. El 75% de los participantes está de acuerdo en que sus organizaciones integran estos riesgos en sus prácticas de TI. El 25% se mantiene neutral.

12. ¿Su institución utiliza actualmente soluciones de IA para la gestión de riesgos en TI?

Gráfico 13. Uso de soluciones de inteligencia artificial en la gestión de riesgos de TI

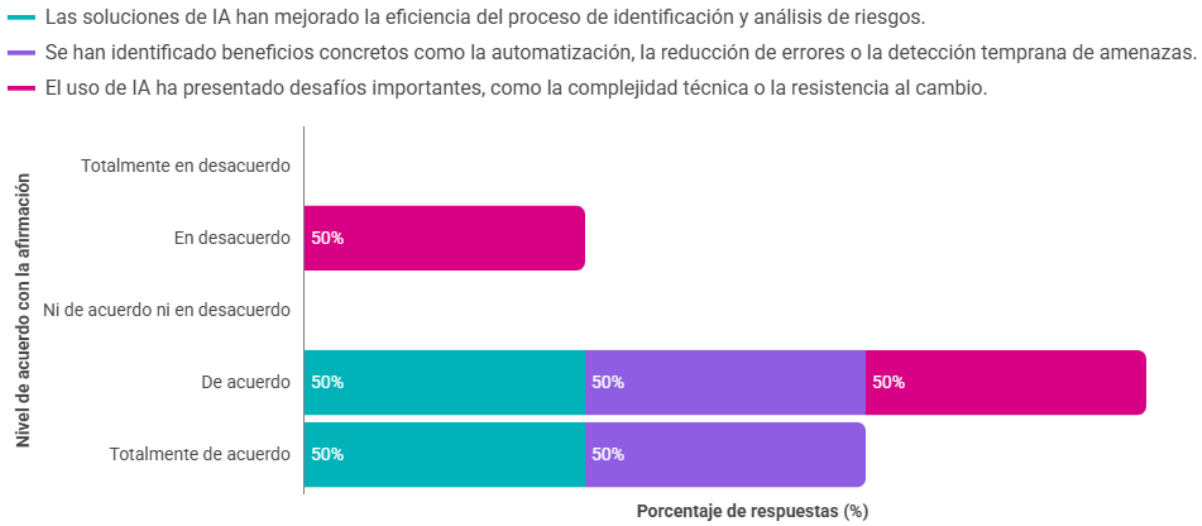


Fuente: Elaboración propia

El 25% de las instituciones utiliza soluciones de inteligencia artificial (IA) para la gestión de riesgos de TI, mientras que el 75% aún no las incorpora. Esto indica que el uso de IA en este ámbito sigue siendo incipiente y no se ha generalizado.

13. En caso de que la pregunta anterior fuese afirmativa, indique su nivel de acuerdo con las siguientes afirmaciones:
    1. Las soluciones de IA han mejorado la eficiencia del proceso de identificación y análisis de riesgos.
    2. Se han identificado beneficios concretos como la automatización, la reducción de errores o la detección temprana de amenazas.
    3. El uso de IA ha presentado desafíos importantes, como la complejidad técnica o la resistencia al cambio.

Gráfico 14. Percepción sobre el impacto del uso de inteligencia artificial en la gestión de riesgos de TI



Fuente: Elaboración propia

Con respecto a las organizaciones encuestadas que usan IA, el 100% está de acuerdo en que la IA mejora la eficiencia en la identificación y análisis de riesgos, con beneficios como automatización y detección temprana de amenazas. Sin embargo, el 50% de ellas no percibe desafíos importantes en la implementación, mientras que el otro 50% sí reconoce problemas como la complejidad técnica y la resistencia al cambio, mostrando que, pese a sus beneficios, la adopción de IA puede enfrentar retos significativos.

Síntesis de hallazgos

Los resultados obtenidos a partir de los instrumentos aplicados proporcionan un diagnóstico actual sobre el estado de la gestión de riesgos en TI en las entidades financieras de carácter local en Costa Rica, sirviendo como insumo estratégico para el diseño y formulación de un manual de buenas prácticas. A continuación, se detallan los principales hallazgos identificados a partir de los resultados de las encuestas y entrevistas.

Hallazgos obtenidos en las encuestas

1. Formalización y cultura de gestión de riesgos
    - El 50 % de las instituciones presenta un nivel moderado de formalización de procesos de gestión de riesgos, evidenciando un amplio margen de mejora en este ámbito. El 89 % documenta los procesos de gestión de riesgos mediante diagramas de flujo.
    - La mayoría de las instituciones, un 62,5 %, percibe la cultura de gestión de riesgos como moderada, lo que indica que hay conciencia sobre la importancia de la gestión de riesgos, pero todavía existen oportunidades de mejora en su implementación y adopción.

2. Identificación, priorización y gobernanza de riesgos
    - En la identificación de riesgos se emplea principalmente el análisis FODA y métricas de desempeño. Para la priorización de riesgos se utilizan mayormente matrices de probabilidad e impacto. Con respecto a los criterios de priorización de los riesgos mayormente se centran en la disponibilidad, consecuencia y capacidad de detección.
    - COBIT 2019 es el marco que más se emplea, seguido de ITIL, mostrando un enfoque robusto en gobernanza de TI.

3. Obstáculos, coordinación y adopción de tecnologías emergentes
    - Solo 37,5 % percibe colaboración efectiva entre la gestión de riesgos de TI con auditoría interna, evidenciando necesidad de mejorar la coordinación y comunicación entre áreas.
    - Los principales obstáculos en la gestión de riesgos son la resistencia al cambio, una cultura organizacional débil en este ámbito y procesos de gestión de riesgos poco estructurados o consolidados.
    - La mayoría de las instituciones, un 75 %, integra activamente riesgos emergentes. Sin embargo, solo un 25 % emplea soluciones de IA, que ofrecen eficiencia y detección

temprana, aunque implican desafíos técnicos y de adaptación, como la resistencia al cambio.

Los hallazgos resultantes muestran que, aunque las instituciones reconocen la importancia de la gestión de riesgos y cuentan con procesos documentados y marcos robustos como COBIT 2019 e ITIL, todavía existe un amplio margen de mejora en formalización, cultura organizacional y colaboración interna. La adopción de tecnologías avanzadas, como la inteligencia artificial, es limitada, y cuando se implementa, enfrenta principalmente obstáculos relacionados con la resistencia al cambio y la complejidad técnica.

Hallazgos obtenidos en las entrevistas

1. Cultura de gestión de riesgos en TI
   La cultura organizacional débil, sumada a la resistencia al cambio y al escaso respaldo de la alta dirección, afecta la incorporación de la gestión de riesgos como parte integral de los procesos. Además, persisten limitaciones como falta de capacitación especializada, escasa alineación entre TI y los objetivos estratégicos del negocio, tercerización, y baja madurez de procesos.

2. Factores clave para fortalecer la cultura de gestión de riesgos
   - Integrar a toda la organización, desde la alta administración hasta los niveles operativos, en la toma de decisiones y en la adopción de buenas prácticas.
   - Incorporar la gestión de riesgos en la planificación estratégica y en la gobernanza corporativa.
   - Asegurar recursos para capacitación continua, manuales actualizados y herramientas seguras que permitan adoptar nuevas tecnologías.

3. Principales desafíos identificados
   - Resistencia al cambio como obstáculo recurrente.
   - Falta de estructuración de los procesos de gestión de riesgos.
   - Limitado apoyo organizacional y presupuestos reducidos.
   - Carencia de personal especializado, especialmente en auditoría de TI.
   - En algunos casos, la cultura organizacional no permea de manera responsable incluso cuando existen recursos.

4. Acciones efectivas para formalizar la gestión de riesgos
    - Establecer una adecuada gobernanza de TI alineada a objetivos estratégicos.
    - Incluir el tema en comités, consejos y juntas directivas con seguimiento anual.
    - Realizar auditorías externas y revisiones conjuntas entre riesgos y auditoría interna.
    - Definir políticas y lineamientos claros, así como roles y responsabilidades.

5. Integración de nuevas tecnologías e inteligencia artificial
    - Estrategias recomendadas: comunicación clara sobre beneficios, capacitación continua, respaldo de la alta administración y definición de proyectos institucionales con objetivos claros.
    - Condiciones necesarias: políticas definidas, herramientas seguras y alineación con la estrategia institucional.

6. Uso de marcos de referencia
    - COBIT 2019 e ITIL son los más utilizados, aunque se reconoce la robustez de ISO 31000 para crear métodos institucionales.
    - Los marcos orientan el “qué hacer” pero no siempre el “cómo”, por lo que se requiere adaptación según el contexto, apetito de riesgo, complejidad y recursos.

7. Buenas prácticas para un sistema efectivo de gestión de riesgos en TI
    - Adopción y adaptación de marcos internacionales (COBIT, ITIL, ISO 31000, ISO 27000, TOGAF).
    - Infraestructura tecnológica robusta, políticas claras y capacitación continua como pilares fundamentales.

Validación de criterio experto

Se contó con el valioso apoyo del Máster Norberto Lee Rodríguez Madrigal, Gerente de TI de la cooperativa de ahorro y crédito Coopealianza R.L, quien posee 27 años de experiencia profesional. Además, es titular de dos maestrías: una en Administración Tecnológica y otra en Auditoría en Tecnología.

El Máster Lee, quien validó la propuesta de solución, recomendó reforzar la inclusión de la primera línea de defensa (Gerencia de TI) en la segunda dimensión, complementando así la segunda línea (gestión de riesgos) y la tercera línea (auditoría interna), y fortalecer la

coordinación entre todas las líneas mediante herramientas que faciliten la comunicación y el acceso a la información.

Para la tercera dimensión, señaló que cada organización define su propia metodología para establecer el apetito de riesgo, considerando la solución propuesta como una alternativa válida de apoyo para la priorización de riesgos.

En la cuarta dimensión, recomendó aprovechar la inteligencia artificial como recurso complementario para enriquecer la gestión de riesgos, asegurando siempre la validación humana, proteger la privacidad de los datos sensibles utilizados y garantizar que las plataformas de IA de terceros mantengan separación y seguridad frente a otros modelos, preservando la integridad de los desarrollos internos. En el Anexo 4 se incluye una minuta que resume las recomendaciones recibidas.

Análisis de brechas

A continuación, en el Cuadro 8, se presenta un resumen del análisis de brechas entre la situación actual de las organizaciones financieras de carácter local y las mejores prácticas establecidas por COBIT 2019 y los lineamientos de la SUGEF. Se emplea la técnica del Hexámetro de Quintiliano como método de apoyo para el desarrollo de la solución.

Cuadro 8. Resumen del análisis de brechas

N°	¿Qué?	¿Quién?	¿Dónde?	¿Cuándo?	¿Por qué?	Buenas prácticas
1	Formalización moderada de los procesos de gestión de riesgos	Colaboradores relacionados con la gestión de riesgos en instituciones financieras locales.	En procesos de gestión de riesgos del área de TI.	Durante encuestas.	Procesos que necesitan ser fortalecidos	APO12.01, APO12.03, APO12.04
2	Cultura de gestión de riesgos moderada o débil	Colaboradores de TI	En el área de TI.	Durante encuestas y entrevistas.	Falta de sensibilización o capacitación	APO12.04 SUGEF - Art. 8
3	Colaboración limitada entre gestión de riesgos de TI y auditoría interna	Equipos de gestión de riesgos de TI y auditoría interna.	En la articulación de las líneas de defensa.	Durante encuestas	Falta de herramientas comunes	Principios de Bartz MEA01.01 SUGEF - Art.8 y Art. 11

4	Oportunidad de mejora en la priorización de riesgos	Gerente de TI, gestión de riesgos	En procesos de evaluación y calificación de riesgos.	Durante encuestas	Oportunidad de mejora en la aplicación de metodología multicriterio	Análisis y clasificación de factores de riesgo de TI utilizando el enfoque basado en TOPSIS difuso (Revisión de literatura)
5	Baja adopción de Inteligencia Artificial en la gestión de riesgos	Organizaciones participantes del estudio.	En procesos de análisis y evaluación de riesgos emergentes.	Durante encuestas y entrevistas.	Resistencia al cambio.	Revisión de literatura - El papel de la tecnología de inteligencia artificial en la evaluación predictiva de riesgos para la continuidad del negocio SUGEF - Art.17

Fuente: Elaboración propia.

CAPÍTULO 5. SOLUCIÓN DEL PROBLEMA

MANUAL DE BUENAS PRÁCTICAS

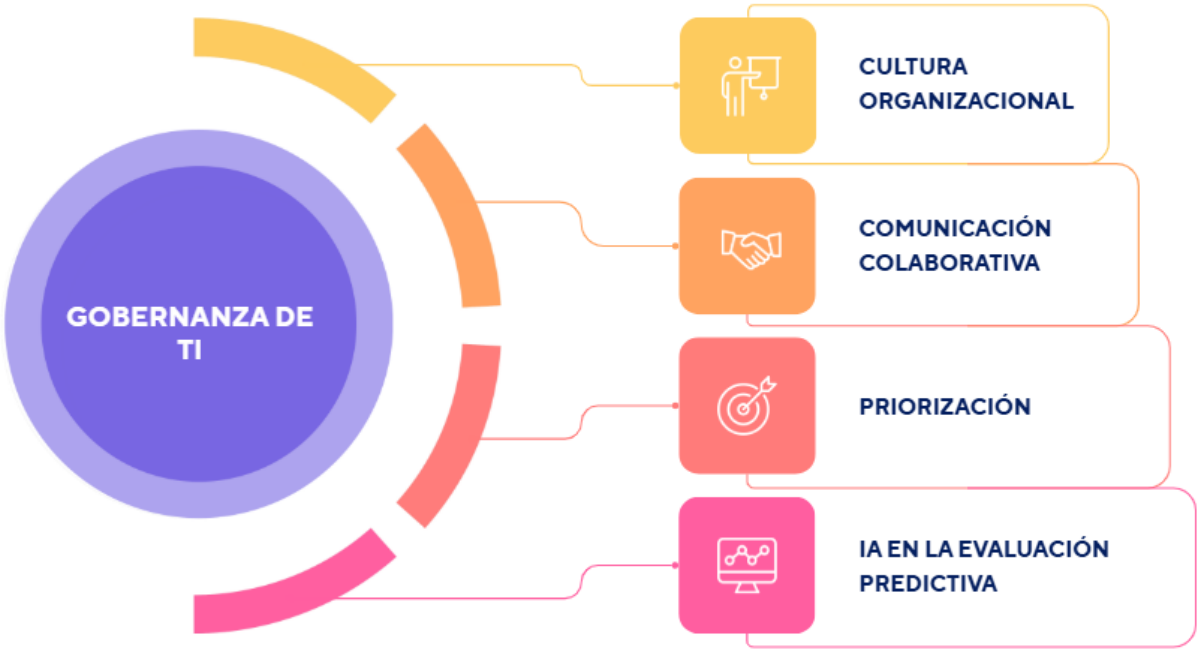
PARA LA GESTIÓN DE RIESGOS EN TECNOLOGÍAS DE LA INFORMACIÓN

Dirigido a organizaciones financieras de carácter local en Costa Rica

Propuesta de solución

El presente manual de buenas prácticas ofrece una guía clara y estructurada para fortalecer procesos de gestión de riesgos de TI en instituciones financieras de carácter local en Costa Rica. La propuesta de solución se construye a partir de los hallazgos del análisis de brechas y se organiza en un eje principal acompañado de cuatro dimensiones independientes. A continuación, se presenta el diagrama cero, el cual constituye la base para el fortalecimiento integral de estos procesos.

Figura 7. Diagrama 0, Propuesta de solución.



Fuente: Elaboración propia

Justificación del enfoque

La gobernanza de TI se establece como el eje principal, ya que constituye el marco que orienta la gestión de riesgos en las organizaciones financieras de carácter local. En las entidades analizadas, dicha gobernanza se refleja principalmente en la adopción de marcos de referencia internacionales, siendo COBIT 2019 el más utilizado. Sin embargo, el nivel de formalización de los procesos se considera moderado, lo que evidencia la existencia de prácticas definidas, aunque aún susceptibles de consolidación y mejora continua. A partir de este eje principal se derivan cuatro dimensiones fundamentales que guían el fortalecimiento de la gestión de riesgos en TI (ver Figura 7), las cuales se describen a continuación.

La primera dimensión, denominada “Cultura organizacional”, se incluye debido a que el 62,5 % de las instituciones encuestadas percibe la cultura de gestión de riesgos en un nivel moderado, siendo “Muy fuerte” el nivel más alto alcanzable. Para fortalecer esta dimensión, se incorporan tres fases estratégicas: sensibilización, capacitación y consolidación (ver Figura 7).

El segundo cuadrante corresponde a la dimensión “Comunicación colaborativa”, la cual se incorpora debido a que únicamente el 37,5 % percibe una colaboración efectiva entre la gestión de riesgos de TI y la auditoría interna. Este resultado evidencia la necesidad de fortalecer la coordinación y los mecanismos de comunicación entre áreas. La propuesta de solución se basa en cuatro principios fundamentales: cultura de apoyo, perfiles en forma de ‘T’, efectividad de los controles y herramientas comunes.

El tercer cuadrante corresponde a la dimensión “Priorización”. Se incluye esta vertical porque, el 89 % de las organizaciones encuestadas que priorizan riesgos utilizan matrices de probabilidad e impacto. Para ofrecer una alternativa, se opta por simplificar el método TOPSIS difuso, empleando los criterios más utilizados por estas organizaciones. La solución para esta dimensión se organiza en tres fases: definición de criterios, evaluación de riesgos y priorización de riesgos.

El cuarto cuadrante corresponde a la dimensión llamada “IA en la evaluación preventiva”, se decide agregar esta dimensión porque solo un 25 % de las instituciones abarcadas emplea soluciones basadas en inteligencia artificial, lo que representa una oportunidad de mejora. Por tanto, la gobernanza de TI debe facilitar la adopción gradual de estas tecnologías.

Desarrollo de la solución

Descripción

El presente manual constituye una guía estructurada para el desarrollo de una solución orientada al fortalecimiento de la gestión de riesgos de Tecnologías de la Información (TI) en organizaciones financieras de carácter local. Se fundamenta principalmente en el marco de referencia COBIT 2019, reconocido por proporcionar principios, componentes y prácticas de gobernanza y gestión de TI alineados con los objetivos estratégicos del negocio, junto con los lineamientos establecidos por el Acuerdo SUGEF 2-10, Reglamento sobre Administración Integral de Riesgos (artículos 8, 11 y 17).

Con base en lo anterior, se busca establecer un enfoque integral que permita a las organizaciones evolucionar desde la sensibilización hasta la consolidación de una cultura organizacional, al mismo tiempo que se promueve la colaboración efectiva entre la gestión de riesgos y la auditoría interna, se priorizan los riesgos mediante criterios objetivos y se incorpora progresivamente la inteligencia artificial (IA) en la evaluación predictiva de riesgos.

Propósito

Proporcionar un manual de buenas prácticas que permita a las organizaciones financieras locales fortalecer su capacidad de gestión de riesgos de TI, mediante la aplicación de buenas prácticas fundamentadas en COBIT 2019. Se pretende que este documento sirva como instrumento de apoyo para los equipos de TI, gestión de riesgos, auditoría interna y alta dirección, facilitando la comunicación, coordinación y toma de decisiones. Además, busca impulsar la madurez organizacional mediante la mejora continua, la capacitación del talento humano y la adopción de IA.

Alcance

El alcance de este manual comprende el diseño y desarrollo de una solución integral dividida en cuatro dimensiones:

1. Cultura organizacional: constituye un proceso cíclico de sensibilización, capacitación y consolidación que fomenta la conciencia y el compromiso con la gestión de riesgos.

2. Comunicación colaborativa: establece lineamientos para fortalecer la interacción entre la gestión de riesgos y la auditoría de TI, promoviendo transparencia, coordinación y una cultura de apoyo mutuo.

3. Priorización: propone un procedimiento estructurado basado en criterios múltiples para clasificar y jerarquizar los riesgos de TI.

4. Inteligencia Artificial en la evaluación predictiva: plantea buenas prácticas para el uso del Procesamiento de Lenguaje Natural (PLN) como herramienta analítica para anticipar riesgos y mejorar la toma de decisiones.

Eje principal: Gobernanza de TI

1. Alinear TI con los objetivos, estrategia y cultura de la organización mediante políticas y prácticas que vinculen la gestión de riesgos con la toma de decisiones y la planificación estratégica.
2. Garantizar la comunicación oportuna de la información sobre riesgos de TI y su gestión a todas las partes interesadas, a través de reuniones estratégicas, promoviendo una cultura organizacional consciente y responsable frente al riesgo.
3. Fortalecer competencias de liderazgo en los equipos de TI, mediante capacitación, mentoría y participación en la toma de decisiones estratégicas relacionadas con riesgos tecnológicos, fomentando la responsabilidad y la rendición de cuentas dentro del área.
4. Impulsar el liderazgo dentro del área de TI, mediante la orientación y motivación de los responsables de cada proceso para que asuman la gestión de riesgos como parte de sus funciones y guíen a sus equipos en la identificación y mitigación de riesgos.

A continuación, se detalla cada dimensión, la cual incluye su descripción general, objetivo, propósito, alcance y las buenas prácticas recomendadas para su aplicación.

Dimensión 1: Cultura organizacional

Descripción general

Esta dimensión se centra en fomentar una mentalidad y un comportamiento organizacional orientados a la gestión efectiva de riesgos de TI. Se desarrolla a través de tres fases que en conjunto conforman un proceso continuo de mejora (ver Figura 8). Se fundamenta en la práctica de gestión denominada ‘APO12.04 - Articular el riesgo’ del marco COBIT 2019, la cual establece la importancia de comunicar oportunamente información sobre exposiciones y oportunidades relacionadas con tecnologías de la información y su impacto en la organización.

Objetivo

Fomentar una cultura organizacional que valore y practique la gestión de riesgos de TI de manera efectiva, mediante la sensibilización de las partes interesadas, el desarrollo de competencias específicas del personal y la institucionalización de buenas prácticas que permitan una mejora continua.

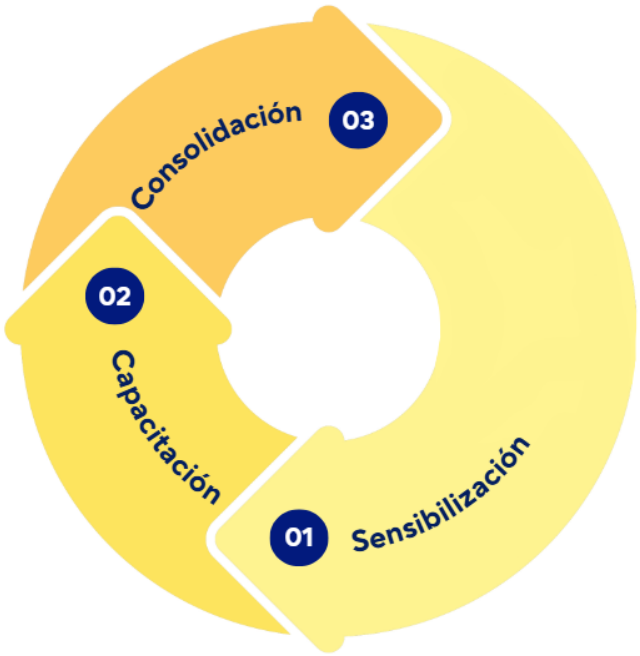
Propósito

Garantizar que la organización cuente con un marco cultural sólido que permita comprender, comunicar y gestionar los riesgos de TI, asegurando que la información sobre riesgos se utilice de manera efectiva en la toma de decisiones estratégicas y operativas.

Alcance

Esta dimensión abarca a todas las áreas y niveles de la organización que participan en procesos relacionados con la gestión de riesgos de TI. Incluye la implementación de actividades de sensibilización, capacitación y consolidación, así como la creación de canales de comunicación, mecanismos de retroalimentación, análisis de incidentes y seguimiento de la efectividad de los controles adoptados. El alcance se extiende desde la alta dirección hasta el personal operativo, promoviendo la adopción de prácticas consistentes y sostenibles en toda la organización.

Figura 8. Fases de fortalecimiento



Fuente: Elaboración propia.

Por cada fase se incluyen actividades para su respectiva implementación. A continuación, se describen en detalle.

Fase 1. Sensibilización

La fase inicial tiene como objetivo fomentar la conciencia y comprensión sobre la importancia de la gestión de riesgos de TI entre todas las partes interesadas, asegurando que la información sea recibida, comprendida y utilizada eficientemente. Esta fase sienta las bases para la siguiente etapa, al generar el conocimiento y la disposición necesarios para participar activamente en los procesos de capacitación.

1.1. Establecer canales de comunicación efectivos mediante la implementación de plataformas o herramientas colaborativas que aseguren la difusión oportuna y accesible de la información sobre riesgos a todas las partes interesadas.

1.2. Planificar presentaciones ejecutivas periódicas mediante sesiones destinadas a comunicar el estado de los riesgos y las acciones implementadas, garantizando su adecuada comprensión por parte de la alta dirección.

Fase 2. Capacitación

A partir de la sensibilización alcanzada en la etapa anterior, esta fase tiene como propósito potenciar las competencias del personal en materia de gestión de riesgos de TI, mediante el desarrollo de habilidades técnicas y operativas que permitan la aplicación efectiva de las prácticas establecidas. La capacitación debe incluir componentes teóricos, prácticos y evaluativos, asegurando que los colaboradores puedan trasladar el conocimiento adquirido a escenarios reales de la organización. Los resultados obtenidos en esta etapa constituyen la base para avanzar hacia la consolidación de una cultura organizacional más sólida y madura en gestión de riesgos.

2.1. Desarrollar capacitaciones periódicas mediante la impartición de talleres y charlas, sobre riesgos de TI y su impacto en los objetivos estratégicos del negocio, dirigidas a todo el personal que participa en procesos relacionados con la gestión de riesgos.

2.2. Evaluar y dar seguimiento a la efectividad de la capacitación mediante pruebas de conocimiento y encuestas de retroalimentación, con el fin de identificar brechas de aprendizaje y ajustar los contenidos o metodologías, asegurando que el personal pueda aplicar de manera efectiva los controles de gestión de riesgos de TI correspondientes a su rol.

Fase 3. Consolidación

Como resultado de las fases anteriores, la etapa de consolidación tiene como objetivo reforzar la gestión de riesgos mediante retroalimentación, análisis de incidentes y seguimiento continuo de las medidas adoptadas. Esta etapa aprovecha las competencias adquiridas durante la fase de capacitación para institucionalizar las buenas prácticas y consolidar las lecciones aprendidas, las cuales retroalimentan la fase de sensibilización.

3.1. Establecer mecanismos sistemáticos de retroalimentación, como reuniones periódicas para recoger las experiencias y sugerencias del personal respecto a la gestión de riesgos.

3.2. Analizar incidentes y eventos de riesgo pasados, documentando lecciones aprendidas y aplicando mejoras en los procesos y controles existentes.

3.3. Mantener un seguimiento continuo de la efectividad de las medidas de riesgo adoptadas, asegurando que se mantenga la mejora continua y la adopción de aprendizajes en toda la organización.

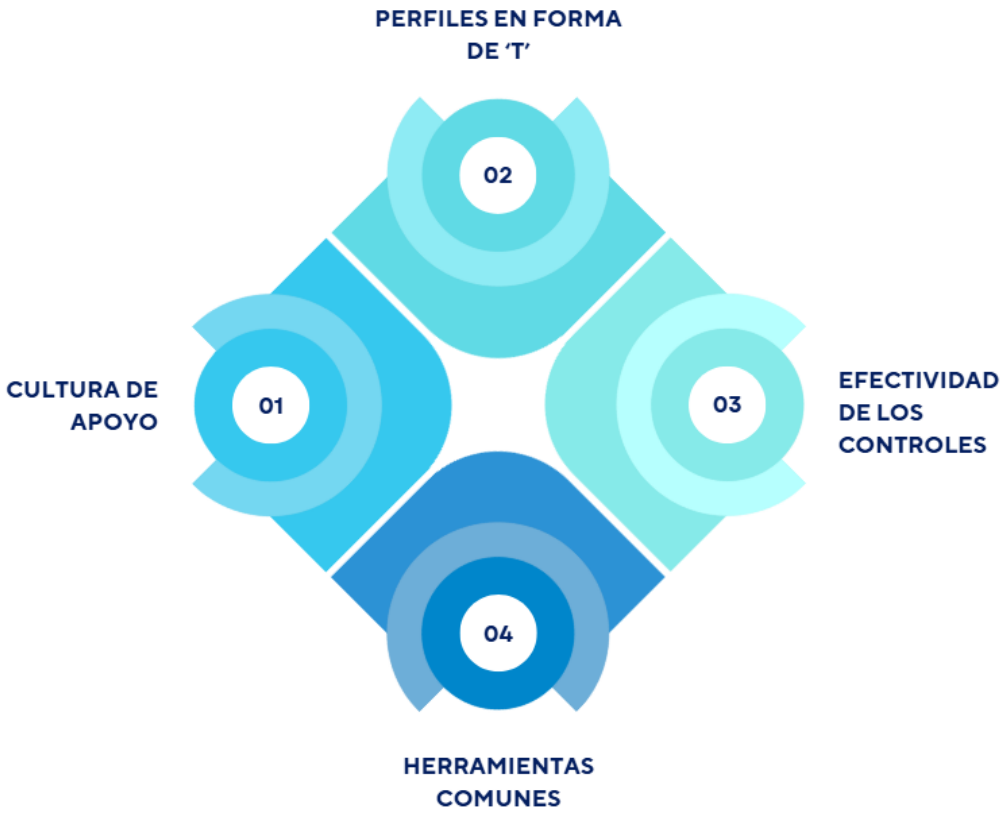
Dimensión 2: Comunicación colaborativa

Descripción general

La efectividad de la gestión de riesgos depende de una comunicación clara y de la colaboración coordinada entre las áreas responsables del control y supervisión. Esta dimensión fortalece la articulación entre el gerente de TI como responsable directo de la operación (primera línea), los equipos de gestión de riesgos como función supervisora (segunda línea) y la auditoría interna de TI como aseguramiento independiente (tercera línea). Su propósito es consolidar una relación sinérgica basada en la confianza, la transparencia y el respeto por las responsabilidades de cada actor.

La propuesta se fundamenta en el modelo de Bartz (2023) y en las buenas prácticas del marco COBIT 2019, con el fin de mejorar la comunicación, evitar duplicidades y promover una visión integral de los riesgos tecnológicos. En la Figura 9 se ilustran los cuatro principios que orientan esta dimensión.

Figura 9. Principios para alianza efectiva entre las principales líneas de defensa.



Fuente: Adaptado de Bartz, B. (2023).

Objetivo

Fortalecer la colaboración entre el gerente de TI, los equipos de gestión de riesgos y la auditoría interna de TI mediante principios y prácticas que promuevan una comunicación efectiva, una adecuada delimitación de responsabilidades y el uso eficiente de herramientas compartidas.

Propósito

Establecer un marco de buenas prácticas que promueva la interacción efectiva y la cooperación entre las líneas de defensa, garantizando independencia, evitando duplicidad de esfuerzos y desarrollando competencias estratégicas y transversales.

Alcance

Estas prácticas aplican al gerente de TI, a la función de gestión de riesgos y a la auditoría interna, así como a todas las unidades organizacionales que intervienen en la ejecución, supervisión o evaluación de controles y riesgos tecnológicos.

Principio 1. Cultura de apoyo

Una cultura de apoyo fomenta la colaboración, el compromiso activo y la alineación de todos los actores organizacionales con los objetivos de riesgo y auditoría. Este principio reconoce además el rol clave de la primera línea de defensa, quien debe promover una cultura de comunicación abierta, reportar oportunamente incidentes y riesgos, y facilitar la coordinación con los equipos de riesgo y auditoría interna.

Para fortalecer esta cultura, se adoptan prácticas de gestión alineadas con el marco COBIT 2019, entre ellas ‘APO07.03 - Mantener las habilidades y competencias del personal’ y ‘APO07.04 - Evaluar y reconocer/recompensar el rendimiento laboral de los empleados’. A continuación, se presentan las prácticas recomendadas.

1.1. Diseñar y ejecutar campañas de comunicación internas mediante boletines, presentaciones, videos educativos y talleres, para informar a toda la organización sobre los alcances, servicios y beneficios de las responsabilidades de la primera línea, la gestión de riesgos y la auditoría de TI.

1.2. Establecer canales de comunicación separados cuando riesgos y auditoría estén bajo la misma estructura organizacional, garantizando que la auditoría conserve su independencia y objetividad, y que la primera línea cuente con rutas claras para reportar incidentes y consultas operativas.

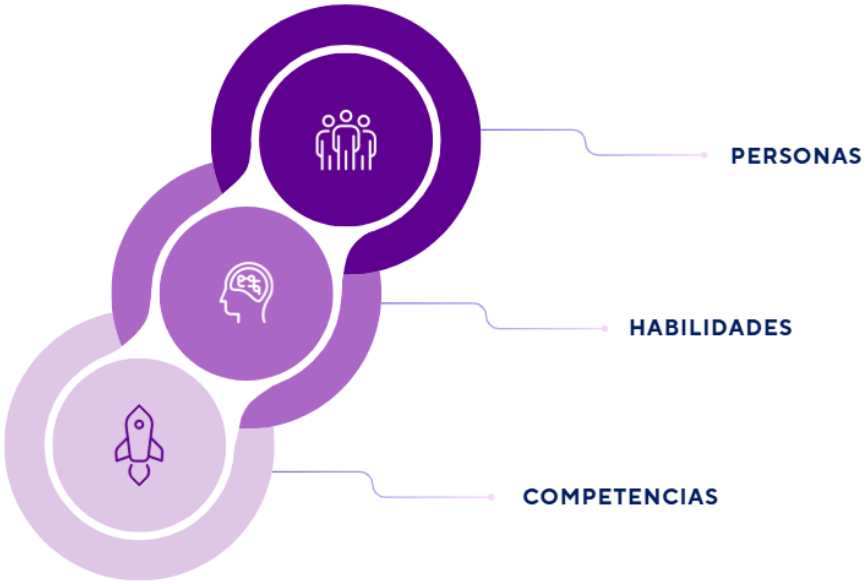
1.3 Implementar sesiones de observación cruzada entre las líneas de defensa, mediante rotaciones breves enfocadas en comprender los procesos, responsabilidades y retos de cada función. Estas experiencias tienen como propósito fortalecer la empatía, la comunicación y la colaboración interdepartamental, sin alterar la independencia funcional de cada equipo.

1.4. Fomentar mecanismos de reconocimiento y retroalimentación entre las líneas de defensa, mediante reuniones periódicas, encuestas de satisfacción y evaluaciones de colaboración, para reforzar la motivación, el aprendizaje compartido y la cultura colaborativa.

Principio 2. Perfiles en forma de ‘T’

Dentro del sistema de gobierno de COBIT 2019, el componente ‘Personas, habilidades y competencias’ (ver Figura 10) constituye la base estratégica para conformar equipos con perfiles en forma de T.

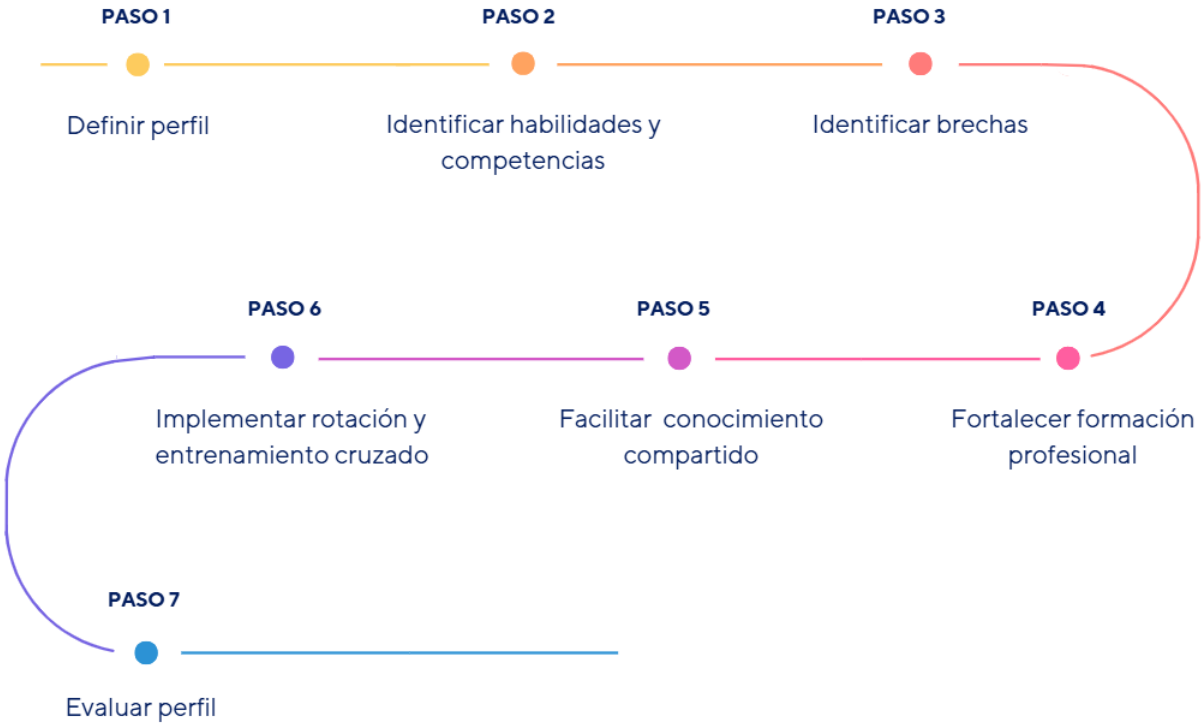
Figura 10. Base estratégica para perfiles en forma de TI.



Fuente: Adaptado, ISACA (2018, p. 13).

Las buenas prácticas que conforman este principio están fundamentadas en ‘APO07.02 - Identificar al personal clave de TI’ y ‘APO07.03 - Mantener las habilidades y competencias del personal’, establecida por el marco COBIT 2019 (ver Figura 11).

Figura 11. Pasos para el desarrollo de perfiles en forma de ‘T’.



Fuente: Elaboración propia.

A continuación, se detalla cada uno de los pasos.

1. Definir formalmente el perfil ideal en forma de 'T' para la primera, segunda y tercera línea de defensa, detallando la profundidad técnica y la amplitud de conocimientos requeridos.
2. Documentar las competencias actuales mediante una matriz de habilidades que relacione al gerente de TI, equipo de gestión de riesgos y auditoría interna con el perfil ‘T’ defino en el Paso 1.
3. Realizar una evaluación periódica para identificar brechas entre las competencias actuales del personal y el perfil ’T’ objetivo.
4. Planificar la carrera profesional de las líneas de defensa, mediante la promoción de certificaciones especializadas en áreas críticas de TI.
5. Facilitar el acceso a repositorios de conocimiento y lecciones aprendidas entre los tres equipos, fomentando el aprendizaje continuo y la mejora de capacidades.
6. Implementar programas de rotación o entrenamiento cruzado en gestión de riesgos y auditoría de TI, que permitan a los profesionales ampliar el dominio técnico y fortalecer la comprensión integral de los procesos, reforzando el perfil en forma de ‘T’.

7. Evaluar periódicamente la pertinencia y actualización del perfil 'T', asegurando que las competencias definidas sigan siendo coherentes con los cambios tecnológicos, normativos y estratégicos de la organización.

Principio 3. El riesgo de TI evalúa adecuadamente la efectividad de los controles

La segunda línea verifica la efectividad de los controles operados por la primera línea manteniendo independencia de auditoría. A continuación, se presentan las prácticas recomendadas.

1. Documentar de forma clara los objetivos, criterios y riesgos de cada control antes de realizar las pruebas, para asegurar que las evaluaciones se hagan de manera ordenada, coherente y fácil de verificar.
2. Fortalecer la supervisión de los controles de TI mediante la definición de indicadores clave de desempeño que permitan identificar los controles más críticos.

Principio 4. Herramientas comunes

Las herramientas comunes permiten colaboración segura y visibilidad integrada entre las líneas de defensa. A continuación, se presentan las prácticas recomendadas.

1. Mantener los registros de evaluaciones de riesgo, controles operados por la gerencia de TI y auditorías en un sistema compartido que ofrezca información actualizada y confiable, evitando duplicación de esfuerzos.
2. Establecer permisos de acceso que permitan compartir únicamente los artefactos que correspondan, asegurando que la información sensible se mantenga confidencial mediante una adecuada gestión de roles y políticas de seguridad de la información.
3. Integrar los resultados de riesgo y los hallazgos de auditoría en dashboards y reportes compartidos en tiempo real, facilitando la toma de decisiones y la visibilidad conjunta de los equipos.

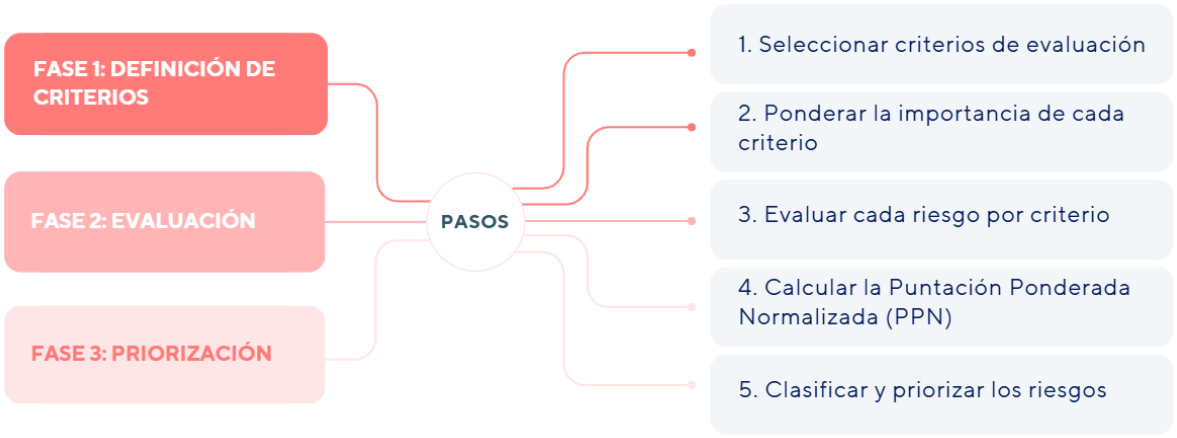
Dimensión 3: Priorización

Descripción general

Esta dimensión se centra en establecer un procedimiento estructurado para clasificar los riesgos de TI según su criticidad y relevancia para la organización. La metodología se fundamentada en la propuesta de Alshahrani et al. (2022), desarrollando una versión simplificada de la misma. Esta utiliza un enfoque de evaluación multicriterio, que permite

considerar tanto factores de costo como de beneficio. El proceso se desarrolla en tres fases: definición de criterios, evaluación y priorización (ver Figura 12).

Figura 12. Fases para la priorización de riesgos



Fuente: Elaboración propia.

Objetivo

Establecer un procedimiento estructurado para clasificar los riesgos de tecnologías de la información según su nivel de criticidad, utilizando un enfoque multicriterio que integre factores de costo y beneficio. Este proceso busca facilitar la toma de decisiones informadas sobre la asignación de recursos y el tratamiento de los riesgos más relevantes.

Propósito

Brindar a organizaciones una herramienta práctica para la toma de decisiones en gestión de riesgos, asegurando que los riesgos más significativos se cuantifiquen y prioricen de manera objetiva, optimizando la eficacia de las medidas de mitigación.

Alcance

La dimensión comprende desde la definición y ponderación de los criterios de evaluación hasta la obtención de un ranking final de riesgos priorizados. Su alcance incluye tanto los riesgos asociados a factores de costo como a factores de beneficio, con el propósito de facilitar un proceso de priorización más integral y objetivo.

A continuación, se detalla el proceso, iniciando con la fase de definición de criterios.

Fase 1: Definición de criterios

Paso 1. Seleccionar criterios de evaluación

1.1. Seleccionar los criterios (C) necesarios que permitan determinar la criticidad del riesgo. Se recomienda considerar los criterios de capacidad de detección, consecuencia, disponibilidad y frecuencia del evento.

1.2. Clasificar cada criterio según su tipo de factor:

- Costo: Una puntuación de 1 (mínima) es más crítica para el riesgo.
- Beneficio: Una puntuación de 5 (máxima) es más crítica para el riesgo.

Paso 2. Ponderar la importancia de cada criterio

2.1. Asignar un peso (P) a cada criterio (C1, C2, C3...) de forma que la suma de todos los pesos sea igual a 1.0. Para la asignación de los pesos por criterio, se recomienda seguir las siguientes actividades:

- Reunir a las personas con mayor conocimiento del riesgo (por ejemplo, gerentes, especialistas en seguridad u otros expertos relacionados).
- Solicitar al grupo que determine el porcentaje de importancia correspondiente a cada criterio.
- Comprobar que la suma total de los porcentajes asignados sea igual a 1.0.
- Solicitar la revisión de un experto adicional para confirmar la consistencia de los resultados y reducir posibles sesgos individuales.

2.2. Elaborar una matriz que incluya, en columnas separadas, el criterio, su definición, el tipo de factor (costo o beneficio) y la ponderación (ver Cuadro 9).

Cuadro 9. Matriz de criterios - Ejemplo

Criterio (C)	Definición	Tipo de factor	Ponderación (P)
C1. Capacidad de detección	Facilidad/rapidez con la que se descubre el evento de riesgo.	Costo	0.20
C2. Consecuencia	Impacto total si el riesgo se materializa.	Beneficio	0.45
C3. Disponibilidad	Grado de afectación al servicio o recurso crítico.	Beneficio	0.15
C4. Frecuencia del evento	Probabilidad de que el evento de riesgo ocurra.	Beneficio	0.20
Resultado			1.0

Fuente: Elaboración propia.

Fase 2: Evaluación

Paso 3. Evaluar cada riesgo por criterio

3.1. Calificar los riesgos que se desean evaluar mediante criterio experto, utilizando la escala definida del 1 al 5, donde la 1 es la más baja y la 5 la más alta para cada uno de los criterios.

3.2. Convertir las puntuaciones directas (PD) a normalizadas (PN) entre 0 y 1 utilizando las siguientes formulas.

El (4) en la formula, representa el rango entre el valor mínimo y máximo. Actúa como un denominador de escala, al dividir por 4, se asegura que el resultado de la normalización siempre esté en el rango de 0 a 1.

- Criterios de beneficio

$$\boldsymbol{PN} = \frac{PD - 1}{4}$$

- Criterios de costo

$$\boldsymbol{PN} = \frac{5 - PD}{4}$$

3.3. Construir una matriz de evaluación que contenga los riesgos en las filas y el resultado de la ponderación normalizada por cada criterio en las columnas (ver Cuadro 10).

Cuadro 10. Matriz de evaluación - Ejemplo

Puntuación Normalizada (PN)				
Riesgo (R)	**C1 - Costo**	**C2 - Beneficio**	**C3 - Beneficio**	**C4 - Beneficio**
R1	(5 - 2) / 4 = **0.75**	(4 - 1) / 4 = **0.75**	(5 - 1) / 4 = **1.00**	(4 - 1) / 4 = **0.75**
R2	(5 - 5) / 4 = **0.00**	(3 - 1) / 4 = 0.50	(4 - 1) / 4 = **0.75**	(5 - 1) / 4 = **1.00**

Fuente: Elaboración propia.

Fase 3. Priorización

Paso 4. Calcular la Puntación Ponderada Normalizada (PPN)

Para cada riesgo, multiplicar la puntación normalizada (PN) por su peso (P) y sumar los resultados.

$$\boldsymbol{PPN_{Riesgo}} = (PN_{C1}\ x\ P_{C1}) + (PN_{C2}\ x\ P_{C2}) + (PN_{C3}\ x\ P_{C3}) + (PN_{C4}\ x\ P_{C4})$$

A continuación, se muestra un ejemplo por cada riesgo.

R1 = (0.75 x 0.20) + (0.75 x 0.45) + (1.00 x 0.15) + (0.75 x 0.20) = **0.7875**

R2 = (0.00 x 0.20) + (0.50 x 0.45) + (0.75 x 0.15) + (1.00 x 0.20) = **0.5375**

Paso 5. Clasificar y priorizar los riesgos

Ordenar los riesgos en orden descendente basándose en la Puntación Ponderada Normalizada (PPN) calculada en el Paso 5. El riesgo con la PPN más ALTA se considera el

más crítico y es el que está más cerca del escenario ideal positivo A* (la peor combinación de resultados). Por lo tanto, se le asigna la prioridad 1 (ver Cuadro 11).

Cuadro 11. Priorización de resultados - Ejemplo

Riesgo (R)	Puntuación Ponderada Normalizada (PPN)	Prioridad
R1	0.7875	1 (Más crítico)
R2	0.5375	2

Fuente: Elaboración propia.

Dimensión 4: IA en la evaluación predictiva

Descripción general

Esta dimensión constituye buenas prácticas para el uso de la inteligencia artificial (IA), en particular el Procesamiento de Lenguaje Natural (PLN), como herramienta de apoyo en la evaluación predictiva de riesgos de TI. Se fundamenta en las prácticas de gestión 'APO07.03 - Mantener las habilidades y competencias del personal', 'APO12.01 - Recopilar datos', 'APO12.03 - Mantener un perfil de riesgo' y 'MEA01.01 - Establecer un enfoque de supervisión', que en conjunto garantizan la calidad de los datos, la actualización continua del perfil de riesgo, la supervisión efectiva de resultados y el fortalecimiento de las capacidades del personal.

Objetivo

Integrar el uso del Procesamiento de Lenguaje Natural (PLN) como componente de apoyo a la evaluación predictiva de riesgos de TI, fortaleciendo la capacidad de anticipación, análisis y respuesta de la organización ante amenazas emergentes.

Propósito

Promover la adopción informada y controlada de soluciones basadas en IA, fortaleciendo la capacidad institucional para anticipar y mitigar riesgos tecnológicos mediante herramientas

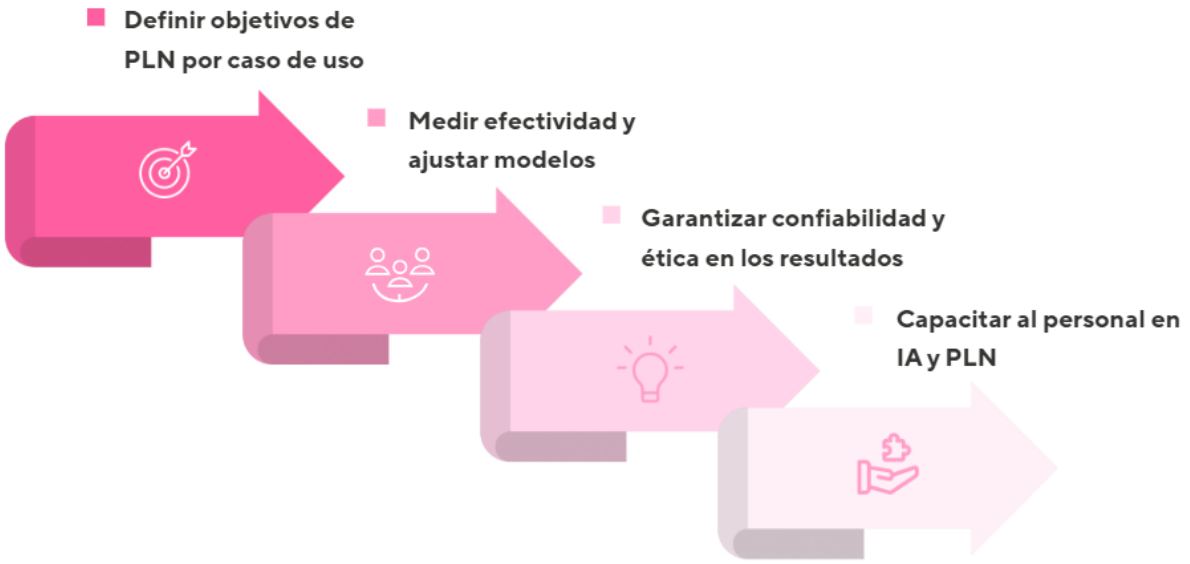
analíticas avanzadas, sin comprometer la integridad, transparencia ni gobernanza del proceso de gestión de riesgos.

Alcance

La dimensión aplica a las organizaciones financieras que consideren integrar el PLN en sus procesos de evaluación predictiva. Su alcance no contempla la implementación técnica directa, sino la definición de prácticas orientadoras para garantizar su adopción responsable y estratégica.

A continuación, se detallan las prácticas recomendadas.

Figura 13. Prácticas para el uso del PLN



Fuente: Elaboración propia.

1. Establecer los fines específicos del uso del PLN mediante la delimitación de casos de aplicación concretos, como la detección temprana de incidentes, el análisis de reportes de auditoría o la identificación de riesgos emergentes. Esto permite enfocar los recursos y garantizar resultados alineados con la estrategia de gestión de riesgos.
2. Garantizar la confiabilidad de los resultados obtenidos por el PLN mediante la validación periódica por parte de analistas y especialistas en riesgo, asegurando trazabilidad y el cumplimiento de principios éticos en el uso de inteligencia artificial.
3. Verificar la efectividad del PLN como parte de una estrategia mediante la aplicación de métricas de evaluación como precisión, cobertura y utilidad de los resultados, ajustando los modelos conforme a las necesidades del entorno organizacional.

4. Fomentar un uso responsable del PLN mediante la formación continua del personal en temas de inteligencia artificial, procesamiento de lenguaje natural y gestión de riesgos tecnológicos.

Procedimiento de implementación

Propósito

Establecer una ruta estructurada para la puesta en marcha de cada una de las dimensiones propuestas en el manual de buenas prácticas para la gestión de riesgos en TI.

Enfoque

El procedimiento se organiza en cuatro fases principales, alineadas con las dimensiones definidas en el manual. Cada fase detalla las actividades a ejecutar, los responsables involucrados, los recursos requeridos, el tiempo estimado en horas y las dependencias existentes entre ellas.

Importancia

El proyecto es de vital importancia y se justifica plenamente al estar fundamentado en COBIT 2019, marco requerido por la SUGEF para el fortalecimiento del gobierno y la gestión de TI. La propuesta de solución atiende puntos débiles identificados en las encuestas y entrevistas realizadas dentro del alcance del estudio. Al fortalecer los procesos y controles mediante una lista de buenas prácticas, el proyecto contribuye a reducir gastos derivados de reprocesos, sanciones y riesgos reputacionales, generando un ahorro significativo y sostenible en el tiempo.

Supuestos

- Los tiempos estimados requeridos para cada actividad se calculan mediante en método PERT y podrán ajustarse conforme al tamaño, la complejidad y el nivel de madurez de la organización.
- Se sugiere una periodicidad para cada actividad, la cual podrá ajustarse según las necesidades operativas de
- Se asume la disponibilidad de un equipo técnico limitado, por lo que se priorizará la eficiencia en la asignación de recursos.
- Se considera que las plataformas o herramientas requeridas para la implementación de determinadas prácticas se fundamenten en software libre.

- La implementación de cada fase podrá implementarse de manera modular conforme a las prioridades estratégicas de la organización.

Roles y responsabilidades

A continuación, en el Cuadro 12 se visualiza los roles y responsabilidades que abarcan la implementación de la solución.

Cuadro 12. Roles y responsabilidades del personal clave en la gestión de riesgos en TI

ID	**Puesto**	**Rol principal**
GER	Gerente de TI	Planificar, dirigir y supervisar la estrategia tecnológica de la organización.
AUD	Auditor interno de TI	Evaluar controles, procesos y cumplimiento de normas en sistemas de información.
ANR	Analista de riesgos de TI	Identificar, evaluar y gestionar riesgos tecnológicos y de información.
SOP	Soporte técnico	Brindar asistencia, mantenimiento y resolución de incidencias de TI.
DGR	Diseñador gráfico	Crear elementos visuales y gráficos para comunicación interna y externa.
RRHH	Recursos humanos	Gestionar talento, contratación, formación y bienestar del personal.
OSI	Oficial de seguridad de la información	Proteger la confidencialidad, integridad y disponibilidad de la información.

Fuente: Elaboración propia.

Eje principal: Gobernanza de TI

Cuadro 13. Implementación del eje principal.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
1	GER	GER	8	12	16	12	12	Anual	N/A
2	GER	GER ANR	4	6	8	6	72	Mensual	1
3	GER	GER	6	9	12	9	9	Anual	1
4	GER	GER	5	8	10	7.83	93.96	Mensual	3
Horas totales estimadas						**34.83**	**186.96**		

Fuente: Elaboración propia.

Dimensión 1. Cultura organizacional

Fase 1. Sensibilización

Cuadro 14. Dimensión 1 - Implementación de la fase inicial

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
1.1	GER	SOP	8	12	20	12.7	-	-	N/A
1.2	GER	ANR	6	10	16	10.3	123.6	Mensual	1.1
Horas totales estimadas						**23**	**123.6**		

Fuente: Elaboración propia.

Fase 2. Capacitación

Cuadro 15. Dimensión 1 - Implementación de la fase intermedia

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
2.1	RRHH	ANR	10	15	24	15.7	31.7	Semestral	1.1 1.2
2.2	RRHH	ANR	6	10	16	10.3	20.6	Semestral	2.1
Horas totales estimadas						**26**	**52.3**		

Fuente: Elaboración propia.

Fase 3. Consolidación

Cuadro 16. Dimensión 1 - Implementación de la fase final

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
3.1	ANR	ANR	6	10	16	10.3	41.2	Trimestral	N/A
3.2	ANR	AUD ANR	8	12	20	12.7	50.8	Trimestral	N/A
3.3	ANR	ANR	6	10	18	10.7	42.8	Trimestral	3.2
Horas totales estimadas						**33.7**	**134.8**		

Fuente: Elaboración propia.

Dimensión 2. Comunicación colaborativa

Principio 1. Cultura de apoyo

Cuadro 17. Dimensión 2 - Implementación del principio 1.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
1.1	ANR	DGR ANR	12	18	28	18.7	37.4	Semestral	N/A
1.2	GER	AUD	6	10	16	10.3	10.3	Anual	N/A
1.3	GER	AUD ANR	8	12	20	12.7	50.8	Trimestral	N/A
1.4	GER	GER	6	10	16	10.3	41.2	Trimestral	N/A
Horas totales estimadas						**52**	**139.7**		

Fuente: Elaboración propia.

Principio 2. Auditoría de TI con perfiles en forma de “T”

Cuadro 18. Dimensión 2 - Implementación del principio 2.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
2.1	GER	RRHH	6	10	16	10.3	-	-	N/A
2.2	GER	GER	8	12	20	12.7	12.7	Anual	2.1
2.3	GER	GER	6	10	16	10.3	10.3	Anual	2.2
2.4	GER	RRHH	8	12	20	12.7	10.3	Anual	2.3
2.5	GER	AUD	4	8	12	8	-	-	N/A
2.6	GER	AUD	6	10	16	10.3	10.3	Anual	N/A
2.7	GER	RRHH	6	10	16	10.3	10.3	Anual	2.4 2.6
Horas totales estimadas						**74.6**	**53.9**		

Fuente: Elaboración propia.

Principio 3. El riesgo de TI evalúa adecuadamente la efectividad de los controles

Cuadro 19. Dimensión 2 - Implementación del principio 3.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
3.1	ANR	ANR	6	10	16	10.3	-	-	N/A
3.2	ANR	ANR	6	10	18	10.7	-	-	3.1
3.3	GER	GER	4	8	12	8	-	-	3.1
Horas totales estimadas						**29**	**-**		

Fuente: Elaboración propia.

Principio 4. Herramientas comunes

Cuadro 20. Dimensión 2 - Implementación del principio 4.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
4.1	GER	ANR AUD	8	12	20	12.7	-	-	N/A
4.2	GER	OSI	6	10	16	10.3	-	-	N/A
4.3	GER	ANR AUD	8	12	20	12.7	-	-	N/A
Horas totales estimadas						**35.7**	**-**		

Fuente: Elaboración propia.

Dimensión 3. Priorización

Este proceso puede aplicarse con la frecuencia que la organización determine necesaria para mantener actualizada su matriz de riesgos.

Fase 1. Definición de criterios

Cuadro 21. Dimensión 3 - Implementación de la fase 1.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
1.1	ANR	ANR	4	6	4	6.3	-	-	N/A
1.2	ANR	ANR	2	4	6	4	-	-	1.1
2.1	ANR	GER AUD ANR OSI	6	10	16	10.3	-	-	1.2
2.2	ANR	ANR	3	5	8	5.3	-	-	2.1
Horas totales estimadas						**25.9**	**-**		

Fuente: Elaboración propia.

Fase 2. Evaluación

Cuadro 22. Dimensión 3 - Implementación de la fase 2.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
3.1	ANR	ANR AUD GER OSI	6	10	16	10.3	-	-	2.2
3.2	ANR	ANR	3	5	8	5.3	-	-	3.1
3.3	ANR	ANR	4	6	10	6.3	-	-	3.2
Horas totales estimadas						**21.9**	**-**		

Fuente: Elaboración propia.

Fase 3. Priorización

Cuadro 23. Dimensión 3 - Implementación de la fase 3.

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
4	ANR	ANR	3	5	8	5.3	-	-	3.3
5	ANR	ANR	2	4	6	4	-	-	4
Horas totales estimadas						**9.3**	-		

Fuente: Elaboración propia.

Dimensión 4. IA en la evaluación predictiva

Cuadro 24. Dimensión 4 - Implementación

No. Actividad	ID Encargado	ID Responsable	O	M	P	TE	TE por año	Periodicidad	Dependencias
4.1	ANR	ANR	4	6	10	6.3	-	-	N/A
4.2	ANR	ANR	6	10	16	10.3	41.2	Trimestral	4.1
4.3	ANR	ANR	6	10	16	10.3	20.6	Semestral	4.2
4.4	RRHH	ANR	4	8	12	8	8	Anual	N/A
Horas totales estimadas						**34.9**	**69.8**		

Fuente: Elaboración propia.

Resumen del tiempo total estimado

El Cuadro 25, presenta el tiempo total estimado por dimensión para la implementación del modelo. En conjunto, las actividades requieren 400,83 horas totales, lo que equivale a 761,06 horas anuales. La dimensión con mayor demanda de tiempo es la dimensión 2, seguida por la dimensión 1.

Cuadro 25. Distribución del tiempo requerido por componente.

Componente	**Horas totales**	**Horas anuales**
Eje central	34.83	186.96
D1: Cultura organizacional	82.7	310.7
D2: Comunicación colaborativa	191.3	193.6
D3: Priorización	57.1	-
D4: IA en la evaluación predictiva	34.9	69.8
Total general	**400.83**	**761.06**

Fuente: Elaboración propia.

CAPÍTULO 6. ANÁLISIS FINANCIERO

Como parte de la validación del Manual de buenas prácticas para la gestión de riesgos de TI en instituciones financieras locales en Costa Rica, se desarrolla un estudio financiero con un periodo de análisis de cinco años. Este análisis se sustenta en una serie de supuestos que se detallan a continuación.

Supuestos

- Debido a las limitaciones que presenta la lista de salarios mínimos publicada por el Ministerio de Trabajo y Seguridad Social para cubrir la totalidad de los puestos analizados, se recurrió al uso de inteligencia artificial (IA) como herramienta complementaria para la estimación salarial. Con este propósito, se diseñó un prompt especializado que permitiera obtener salarios representativos del sector financiero costarricense, tomando como referencia perfiles con una experiencia mínima de cinco años en el año 2025.
- Las cargas sociales patronales son los aportes que la empresa debe pagar sobre el salario de sus colaboradores. Estas incluyen el Seguro de Enfermedad y Maternidad (SEM) con una tasa del 5,50%, el Seguro de Invalidez, Vejez y Muerte (IVM) con un 4,17%, así como las provisiones correspondientes al aguinaldo, vacaciones y cesantía obteniendo un resultado aproximado del 51%. Para efectos de estimación, el cálculo se realiza multiplicando el salario bruto por el porcentaje correspondiente a cargas sociales patronales, y dividiendo el resultado entre doce meses.
- Para estimar el salario por hora de un colaborador, se establecen ciertos supuestos respecto a su jornada laboral. Se considera que el colaborador labora 8 horas diarias durante 5 días a la semana, lo que equivale a un total de 40 horas semanales. Dado que un año cuenta con 52 semanas, el promedio de semanas por mes es de aproximadamente 4,33. Al multiplicar las horas semanales por dicho promedio, se obtiene una estimación de 173,2 horas trabajadas por mes. En consecuencia, el salario por hora de cada colaborador se obtiene dividiendo el costo total, entre el número promedio de horas trabajadas al mes.
- Se considera una tasa de descuento equivalente al 12%.
- No se incluyen supuestos sobre los costos fijos de equipo y mobiliario, dado que estos varían según cada organización

La implementación del manual aporta beneficios directos y verificables en el tiempo, fortaleciendo la gestión de riesgos en TI. A continuación, se detallan los principales beneficios.

Beneficios

- Fortalecimiento de la cultura organizacional, al establecer prácticas claras, consistentes y alineadas con buenas prácticas internacionales.
- Mejor coordinación entre las líneas de defensa, lo que reduce reprocesos, duplicidades y brechas en el control interno.
- Se minimiza el riesgo de multas y sanciones derivadas del incumplimiento de la normativa de la SUGEF, dado que la solución se fundamenta en COBIT 2019.
- Se previene el deterioro de la reputación institucional y la pérdida de confianza de los clientes, que son consecuencias de una gestión de riesgos inmadura o reactiva.

Evaluación del proyecto

Inversión inicial

La inversión inicial de este proyecto considera al menos un colaborador por cada puesto, dado que se trata de instituciones financieras de carácter local. En el Cuadro 26 se presentan las horas totales asignadas a cada colaborador según su puesto, así como el total de horas anuales, la tarifa por hora, el costo de la inversión inicial y los costos anuales correspondientes.

Cuadro 26. Detalle de inversión inicial y costos anuales por puesto

ID Puesto	Horas totales	Horas anuales	Tarifa por hora (¢)	Costo inversión inicial (¢)	Costos anuales (¢)
GER	78.28	215.16	15,053.75	1,178,088.75	3,238,300.29
AUD	59.15	71.40	9,029.04	533,969.80	644,763.46

ANR	187.60	435.20	9,029.04	1,693,248.38	3,929,915.09
SOP	12.70	-	5,416.08	68,784.62	-
DGR	9.35	18.70	5,416.08	50,650.35	101,221.70
RRHH	33.30	20.60	7,223.77	240,517.34	148,709.66
OSI	15.45	-	9,029.04	139,496.07	-
Total	**400.83**	**761.06**	-	**3,954,755.00**	**8,062,910.20**

Se proyecta una inversión inicial de **₵ 3,954,755.00.**

Ingresos

El proyecto no genera ingresos directos, sin embargo, los beneficios obtenidos se traducen en ahorros y costos evitados para las organizaciones. Con el objetivo de monetizar estos beneficios, se detallan a continuación supuestos que ayudan a realizar este análisis.

Ahorros

Esta categoría representa los beneficios obtenidos por la optimización de procesos y el mejor uso del tiempo de los colaboradores.

1. Reducción de reprocesos gracias a procesos estandarizados.
2. Menor tiempo en la coordinación entre áreas, traduciéndose en ahorro de horas laborales.
3. Disminución del tiempo en el análisis de riesgos, al contar con un método eficiente de priorización para la toma de decisiones.
4. Optimización de horas-colaborador en el análisis de grandes volúmenes de información.

Cuadro 27. Supuestos de ahorros

Concepto	Supuesto	Cálculo	Monto anual
Reducción de reprocesos	206,25 horas/año de personal promedio evitadas.	206,25 horas x ₡8,000/hora	1,650,000
Disminución del tiempo en análisis	100 horas/año de analista ahorradas.	100 horas × ₡9,000/hora	900,000
Optimización de horas-colaborador	200 horas/año optimizadas en colaboradores clave.	200 horas x ₡8,000/hora	1,600,000
Total			**4,150,000**

Fuente: Elaboración propia.

Costos evitados

Esta categoría representa el dinero que la organización se ahorra al prevenir eventos negativos o fallas que generarían un gasto, una pérdida, o una sanción.

1. Multas y sanciones regulatorias (SUGEF).
2. Pérdida de reputación por fallos en la gestión de riesgos.
3. Errores o duplicación de esfuerzos en tareas y controles.
4. Pérdidas derivadas de la detección tardía de riesgos emergentes.
5. Impactos financieros o reputacionales por amenazas no anticipadas.

Cuadro 28. Supuestos de costos evitados

Concepto	Supuesto	Cálculo	Monto anual
Multas y sanciones regulatorias	Prevención de al menos una sanción anual equivalente a ₡2,000,000	1 x ₡2,000,000	2,000,000
Pérdidas derivadas de detección tardía	La detección temprana libera 411.76 horas/año de trabajo que habrían sido necesarias para mitigar la pérdida.	411.76 horas × ₡8.500/hora	3,500,000
Total			**5,500,000**

Fuente: Elaboración propia.

Egresos

- Costos fijos: Se incluyen los costos relacionados con el recurso humano.

Cuadro 29. Costos fijos por puesto

Puesto	Salario bruto (¢)	Cargas sociales patronales por mes (¢)	Costo total (¢)	Tarifa estimada por hora (¢)
Gerente de TI	2,500,000	106,250	2,606,250	15,053.75
Auditor interno de TI	1,500,000	63,750	1,563,750	9,029.04
Analista de riesgos de TI	1,500,000	63,750	1,563,750	9,029.04
Soporte técnico	900,000	38,250	938,250	5,416.08
Diseñador gráfico	900,000	38,250	938,250	5,416.08

Recursos humanos	1,200,000	51,000	1,251,000	7,223.77
Oficial de seguridad de la información	1,500,000	63,750	1,563,750	9,029.04

Fuente: Elaboración propia.

- Costos variables: En este estudio, no se contemplan costos variables asociados al proyecto.

Flujo de caja

El proyecto se considera viable y aceptable según los criterios de evaluación financiera. El Valor Actual Neto (VAN) indica que el proyecto es rentable, ya que no solo cubre la totalidad de los costos e inversiones incurridas, sino que además genera una ganancia neta adicional de casi 4 millones de colones. Respecto a la Tasa Interna de Retorno (TIR), el proyecto se califica como aceptable. La rentabilidad real estimada es del 13%, lo que se sitúa 1 punto porcentual por encima de la rentabilidad mínima (tasa de descuento) del 12%. Finalmente, en cuanto al período de recuperación, el Playback (PER) la inversión se recuperará de forma relativamente rápida en un plazo de 3 años y 7 meses, lo cual contribuye a limitar la exposición del capital.

Figura 14. Flujo de caja del proyecto

Parámetros						
Tasa de descuento (K) - Lo que el inversor espera ganar	12%					
Impuesto sobre la renta	30%					
FLUJO DE CAJA						
PERIODO	0	1	2	3	4	5
INGRESOS / BENEFICIOS		CRC 9 650 000,00	CRC 9 650 000,00	CRC 9 650 000,00	CRC 9 650 000,00	CRC 9 650 000,00
Ahorros		CRC 4 150 000,00	CRC 4 150 000,00	CRC 4 150 000,00	CRC 4 150 000,00	CRC 4 150 000,00
Reducción de reprocesos		CRC 1 650 000,00	CRC 1 650 000,00	CRC 1 650 000,00	CRC 1 650 000,00	CRC 1 650 000,00
Disminución del tiempo en análisis		CRC 900 000,00	CRC 900 000,00	CRC 900 000,00	CRC 900 000,00	CRC 900 000,00
Optimización de horas-colaborador		CRC 1 600 000,00	CRC 1 600 000,00	CRC 1 600 000,00	CRC 1 600 000,00	CRC 1 600 000,00
Costos evitados		CRC 5 500 000,00	CRC 5 500 000,00	CRC 5 500 000,00	CRC 5 500 000,00	CRC 5 500 000,00
Multas y sanciones regulatorias		CRC 2 000 000,00	CRC 2 000 000,00	CRC 2 000 000,00	CRC 2 000 000,00	CRC 2 000 000,00
Pérdidas derivadas de detección tardía		CRC 3 500 000,00	CRC 3 500 000,00	CRC 3 500 000,00	CRC 3 500 000,00	CRC 3 500 000,00
EGRESOS		CRC 8 062 910,20	CRC 8 062 910,20	CRC 8 062 910,20	CRC 8 062 910,20	CRC 8 062 910,20
Costos Fijos		CRC 8 062 910,20	CRC 8 062 910,20	CRC 8 062 910,20	CRC 8 062 910,20	CRC 8 062 910,20
Salario Gerente de TI		CRC 3 238 300,29	CRC 3 238 300,29	CRC 3 238 300,29	CRC 3 238 300,29	CRC 3 238 300,29
Salario Auditor interno		CRC 644 763,46	CRC 644 763,46	CRC 644 763,46	CRC 644 763,46	CRC 644 763,46
Salario Analista de riesgos		CRC 3 929 915,09	CRC 3 929 915,09	CRC 3 929 915,09	CRC 3 929 915,09	CRC 3 929 915,09
Salario Soporte técnico		CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00
Salario Diseño gráfico		CRC 101 221,70	CRC 101 221,70	CRC 101 221,70	CRC 101 221,70	CRC 101 221,70
Salario Recursos humanos		CRC 148 709,66	CRC 148 709,66	CRC 148 709,66	CRC 148 709,66	CRC 148 709,66
Salario Oficial de seguridad de información		CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00
Costos Variables		CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00
-		CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00	CRC 0,00
Utilidad o pérdida antes de impuestos		CRC 1 587 089,80	CRC 1 587 089,80	CRC 1 587 089,80	CRC 1 587 089,80	CRC 1 587 089,80
Impuesto sobre la renta		CRC 476 126,94	CRC 476 126,94	CRC 476 126,94	CRC 476 126,94	CRC 476 126,94
Utilidad o pérdida después de impuestos		CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86
Flujo Neto despues de Impuestos (ING-EGR-IMPUESTOS)		CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86
INVERSIÓN INICIAL	-CRC 3 954 755,00					
Eje central	CRC 447 219,08					
Dimensión 1	CRC 824 432,88					
Dimensión 2	CRC 1 950 576,84					
Dimensión 3	CRC 515 645,02					
Dimensión 4	CRC 216 881,18					
Flujo neto en efectivo	-CRC 3 954 755,00	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86	CRC 1 110 962,86
Flujo de caja acumulado	-CRC 3 954 755,00	-CRC 2 843 792,14	-CRC 1 732 829,28	-CRC 621 866,42	CRC 489 096,44	CRC 1 600 059,30
Factor de descuento		0,89	0,80	0,71	0,64	0,57
Flujo neto descontado	-CRC 3 954 755,00	CRC 1 244 278,40	CRC 1 393 591,81	CRC 1 560 822,83	CRC 1 748 121,57	CRC 1 957 896,16
VAN	CRC 3 949 956					
TIR	13%					
Periodo de recuperacion:						
Año negativo	3					
Fraccion año positivo	0,56					
Año de recuperación	3,56					

Fuente: Elaboración propia.

CAPÍTULO 7. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Según el alcance definido y la muestra recolectada:

- La formalización en general de los procesos de gestión de riesgos de TI presenta un nivel de madurez moderado, dado que solo la mitad de las instituciones considera haber alcanzado un nivel alto de formalización. Esta situación evidencia los puntos débiles identificados en las organizaciones financieras de carácter local, por lo que se propone fortalecer cada uno mediante la incorporación de buenas prácticas fundamentadas en el marco de gestión COBIT 2019 y lineamientos de la SUGEF.
- El principal obstáculo para una gestión de riesgos efectiva no radica en la ausencia de marcos de referencia, dado que se identificó que la gestión de riesgos se apoya en COBIT 2019 e ITIL, sino en barreras humanas, como la resistencia al cambio y una cultura organizacional débil.
- Existe una brecha significativa en la coordinación entre las líneas de defensa, dado que únicamente una minoría de las organizaciones percibe una colaboración efectiva entre gestión de riesgos y auditoría interna.
- El uso de soluciones de IA para la gestión de riesgos de TI es mínimo, dado que la mayoría de las organizaciones evaluadas aún no aplican esta tecnología. En consecuencia, el PLN no se utiliza de manera generalizada en el sector, lo que constituye una oportunidad de mejora para las organizaciones que decidan adoptarla.
- La IA debe considerarse un recurso complementario y no sustitutivo. Es imprescindible que el criterio humano se mantenga como control principal, garantizando la rendición de cuentas y mitigando riesgos éticos o sesgos en los resultados de los modelos algorítmicos.
- El manual de buenas prácticas es un producto final pertinente y aplicable que provee una solución metodológica concreta, validada por expertos del sector, para subsanar las debilidades diagnosticadas y fortalecer la gestión de riesgos de TI.

Recomendaciones

- Se recomienda a los gerentes de TI establecer un proceso de revisión continua del manual de buenas prácticas propuesto, que incluya actualizaciones periódicas basadas en cambios regulatorios, incorporación de nuevas tecnologías y lecciones aprendidas de incidentes o auditorías. Esto asegurará que el manual siga siendo un referente confiable y práctico para la organización, fortaleciendo la gestión de riesgos, promoviendo la adopción consistente de buenas prácticas y manteniendo la alineación con los estándares del sector.
- Se recomienda a los gerentes de TI establecer métricas específicas para evaluar el desempeño de cada componente de la propuesta de solución, con el fin de medir de manera objetiva el cumplimiento de las prácticas establecidas, identificar oportunidades de mejora y respaldar la toma de decisiones basada en resultados.
- Se recomienda a las cooperativas de ahorro y crédito locales invertir y facilitar estratégicamente el uso de soluciones de IA como apoyo para la evaluación predictiva de riesgos de TI, aprovechando su capacidad de analizar grandes volúmenes de datos, identificar patrones y anticipar incidentes. No obstante, el criterio humano debe mantenerse como control principal, asegurando que las decisiones sean transparentes y responsables.
- Se recomienda a futuros investigadores profundizar en el bajo nivel de adopción de la IA en la gestión de riesgos de TI en las cooperativas de ahorro y crédito locales en Costa Rica, ya que es importante comprender por qué, pese a su potencial, esta tecnología no se utiliza de manera generalizada en el sector financiero.
- Se recomienda a los encargados de la gestión del riesgo de las organizaciones financieras de carácter local, automatizar la “Dimensión 3: Priorización” mediante una hoja de cálculo estructurada en Excel. Esta herramienta debe incluir criterios, ponderaciones y fórmulas integradas en esta dimensión que permitan calcular automáticamente el nivel de criticidad de cada riesgo. Además, se sugiere habilitar su acceso para las líneas de defensa y las áreas involucradas en el proceso, de manera que se facilite la actualización continua, la trazabilidad y la toma de decisiones basada en información centralizada.

En caso de implementar IA:

- Se recomienda a los gerentes de TI implementar soluciones tecnológicas integrales que permitan una comunicación fluida y el acceso centralizado a información relevante entre todas las líneas de defensa abarcadas. Esto incluye plataformas de colaboración, tableros de seguimiento y sistemas de alerta temprana que fortalezcan la coordinación operativa, reduzcan retrasos en la toma de decisiones y garanticen un flujo de información constante, seguro y transparente entre gestión de riesgos, auditoría interna y otras áreas clave para la operación y la toma de decisiones estratégicas.
- Se recomienda a los oficiales de seguridad de la información de las cooperativas de ahorro y crédito locales, garantizar la privacidad, seguridad e integridad de los datos utilizados en los modelos de IA, considerando que la información suele ser confidencial, interna o de acceso restringido. Para ello, se deben establecer políticas y controles que aseguren su manejo adecuado, y supervisar que las plataformas de terceros mantengan una separación clara de otros modelos, protegiendo la exclusividad y confidencialidad de los desarrollados internamente.

CAPÍTULO 8. ANÁLISIS RETROSPECTIVO

La MATI fue una etapa profundamente significativa en mi vida. Más que un proceso formativo, representó una experiencia de crecimiento, disciplina y autoconocimiento. Además, me permitió construir relaciones de amistad que dejaron una huella en mi camino.

Como ingeniera en sistemas graduada de la Universidad Nacional, con experiencia sobre todo en desarrollo de software y control de calidad, la maestría abrió para mí un mundo completamente nuevo. Trabajar en un proyecto sobre la gestión de riesgos de TI significó adentrarme en un tema que no formaba parte de mi experiencia previa. Ese reto se convirtió en uno de los aprendizajes más significativos, al implicar la comprensión y aplicación de conceptos y metodologías distintas a las que estaba familiarizada.

Además, me brindó herramientas esenciales que fortalecieron no solo mis competencias técnicas, sino también las estratégicas y humanas. Recuerdo especialmente los cursos enfocados en liderazgo, gestión del tiempo, resolución de conflictos, comunicación y habilidades blandas, los cuales considero especialmente valiosos en mi desarrollo profesional y personal.

La maestría amplió mi visión sobre el papel que puedo desempeñar dentro de una organización. Me permitió descubrir nuevas habilidades que no conocía. Para mí, finalizar esta etapa no representa un cierre, sino un punto de partida que me invita a seguir explorando y ampliando mis capacidades, descubriendo que puedo ir más allá de lo que imaginaba.

Como reflexión final, me quedo con las palabras de Zig Ziglar, reconocido motivador y conferencista en desarrollo personal, éxito, ética laboral y liderazgo: “El logro de un objetivo no es tan importante como la persona en la que te conviertes al alcanzarlo”, una idea que resume perfectamente la esencia de esta etapa de mi vida.

Referencias bibliográficas

Nikolaenko, V., & Sidorov, A. (2023). Analysis of 105 IT Project Risks. Journal of Risk & Financial Management, 16(1), 1–20.

Ivanova, R. (2021). ISO 31000 - Prerequisite for Strategic Risk Management in the Activities of Organizations. Izvestia Journal of the Union of Scientists - Varna. Economic Sciences Series, 10(1), 55–62.

Superintendencia General de Entidades Financieras. (s.f.). Objetivos y funciones. Superintendencia General de Entidades Financieras. Obtenido en: https://www.sugef.fi.cr/sugef/objetivos_funciones.aspx

Superintendencia General de Entidades Financieras. (2025). Lista de entidades fiscalizadas por la SUGEF (julio 2025). Obtenido en: https://www.sugef.fi.cr/ver/entidades_supervisadas/lista_entidades_supervisadas/entidades_fiscalizadas/2025/2025_05.pdf

Acebes, F., González-Varona, J. M., López-Paredes, A., & Pajares, J. (2024). Beyond probability-impact matrices in project risk management: A quantitative methodology for risk prioritisation. Humanities & Social Sciences Communications, 11(1), 1–13. https://doi.org/10.1057/s41599-024-03180-5

International Organization for Standardization. (2018). ISO 31000:2018: Gestión del riesgo - Directrices. ISO. Obtenido en: https://www.iso.org/standard/65694.html

ISACA. (2018). Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión. Obtenido en: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko99EAC

Superintendencia General de Entidades Financieras. (2024, 1 de enero). Acuerdo SUGEF 2-10 (v. 29): Reglamento sobre administración integral de riesgos. Consejo Nacional de Supervisión del Sistema. Obtenido en: https://www.sugef.fi.cr/normativa/normativa_vigente.aspx

Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF). (2024, 22 de julio). Acuerdo CONASSIF 5-24: Reglamento general de gobierno y gestión de la tecnología de información. La Gaceta, Alcance 130 a La Gaceta 134. Obtenido en: https://www.sugef.fi.cr/normativa/NormativaTransversal.aspx

Medina Romero, M. A., Rojas León, C. R., Bustamante Hoces, W., Loaiza Carrasco, R. M., Martel Carranza, C. P., & Castillo Acobo, R. Y. (2023). Metodología de la investigación: Técnicas e instrumentos de investigación. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú.

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill Education.

Callow Monge, A. (2021). Elaboración de una propuesta de herramientas y procedimientos para la evaluación de desempeño del personal y del clima organizacional y una valoración del manual de puestos de la empresa Tico Electronics (Tesis de bachillerato). Tecnológico de Costa Rica, Campus Tecnológico Local San José.

Herrera Madriz, F. (2024). Propuesta de Metodología para la Gestión de Riesgos de TI Basada en las Mejores Prácticas Internacionales para la Empresa Information Evolution Costa Rica. Instituto Tecnológico de Costa Rica.

Alshahrani, H. M., Alotaibi, S. S., Ansari, M. T. J., Asiri, M. M., Agrawal, A., Khan, R. A., Mohsen, H., & Hilal, A. M. (2022). Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. Applied Sciences, 12(12), 5911. https://doi.org/10.3390/app12125911

Bartz, B. (2023). IT Risk and IT Audit Working Together to Reduce the Burden on the Business. ISACA Journal, 5, 20–23. https://www.isaca.org/

Almasria, N. A., Ershaid, D. J., Jalghoum, Y. A., & Almajali, A. F. (2025). The role of FinTech in transforming risk management and financial services: A systematic review and meta-analysis. Financial and Credit Activity: Problems of Theory and Practice, 2(61), 409–424. https://doi.org/10.55643/fcaptp.2.61.2025.4698

Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., & Chatzitheodoridis, F. (2024). The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece. Risks, 12(2), 1–23.
Bartz, B. (2023). IT Risk and IT Audit Working Together to Reduce the Burden on the Business. ISACA Journal, 5, 20-23.

Toro, R., Peña-Sarmiento, M., Avendaño-Prieto, B. L., Mejía-Vélez, S., & Bernal-Torres, A. (2022). Análisis empírico del coeficiente alfa de Cronbach según opciones de respuesta,

muestra y observaciones atípicas. Revista Iberoamericana de Diagnóstico y Evaluación – e Avaliação Psicológica (RIDEP), 63(2), 17-30. https://doi.org/10.21865/RIDEP63.2.02

Leonard. (2023, February 8). How to calculate Cronbach's Alpha in Excel. *Uedufy*. https://uedufy.com/how-to-calculate-cronbachs-alpha-in-excel/

Deloitte. (2020). *Modernizing the three lines of defense model: An internal audit perspective*. Deloitte. https://www.deloitte.com/us/en/services/consulting/articles/modernizing-the-three-lines-of-defense-model.html

Bagshaw, K. B. (2021). PERT and CPM in Project Management with Practical Examples. American Journal of Operations Research, 11, 215-226. https://doi.org/10.4236/ajor.2021.114013

Sapag Chain, N., Sapag Chain, R., & Sapag Puelma, J. M. (2014). *Preparación y evaluación de proyectos* (6a ed.). McGraw Hill Education.

Financial Services Regulatory Authority of Ontario (FSRA). (2024). *Information Technology ("IT") risk management*. Recuperado de https://www.fsrao.ca/information-technology-it-risk-management

Glosario

1. **APO** (Alinear, Planificar y Organizar): Dominio de objetivos de gestión en el marco de referencia COBIT 2019, que aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología (ISACA, 2018).
2. **COBIT** (Control Objectives for Information and Related Technology): Es un marco de referencia creado por ISACA para la gobernanza y gestión de TI (ISACA, 2018).
3. **CONASSIF** (Consejo Nacional de Supervisión del Sistema Financiero) en Costa Rica.
4. **DSS** (Entregar, Dar Servicio y Soporte): Dominio de objetivos de gestión en el marco de referencia COBIT 2019, que aborda la entrega operativa y el soporte de los servicios de información y tecnología, incluida la seguridad (ISACA, 2018).
5. **EDM** (Evaluar, Dirigir y Monitorizar): Dominio de objetivos de gobierno en el marco de referencia COBIT 2019 (ISACA, 2018).
6. **ISO 31000**: Norma que define los principios básicos y las directrices para la gestión de riesgos a los que se enfrentan las organizaciones, independientemente de su tamaño o tipo de entidad (ISO, 2018).
7. **MEA** (Monitorizar, Evaluar y Valorar): Dominio de objetivos de gestión en el marco de referencia COBIT 2019, que aborda la monitorización del rendimiento y la conformidad de I&T (ISACA, 2018).
8. **PERT** (Técnica de Evaluación y Revisión de Programas): Método que realiza tres estimaciones de tiempo para cada actividad, asumiendo una distribución de probabilidad beta, y permite reflejar de manera más realista la incertidumbre asociada a actividades con duraciones indeterminadas (Bagshaw, 2021).
9. **SUGEF** (Superintendencia General de Entidades Financieras): Organismo encargado de supervisar y regular entidades financieras en Costa Rica.
10. **TI** (Tecnología de Información).

Anexos

Anexo 1. Entrevista N.° 1: Profesional en gestión de riesgos en TI

Asunto	Entrevista enfocada en la gestión de riesgos en TI			**Responsable**	Ivannia Rojas Gutiérrez
Modalidad	Vía zoom	**Hora inicio**	04:00 pm		
Fecha	05/08/2025	**Duración total**	20 minutos	**Entrevista N.°**	1

Resumen de hallazgos

1. Uno de los hallazgos obtenidos a partir de la encuesta aplicada en instituciones financieras de carácter local en Costa Rica indica que la cultura de gestión de riesgos en el área de tecnologías de la información (TI) es percibida como moderada por los encuestados.

   1.1 ¿Qué factores considera que limitan actualmente el desarrollo de una cultura sólida de gestión de riesgos en TI dentro una organización?

   La limitada capacitación en gestión de riesgos en tecnologías de la información se considera uno de los principales factores que obstaculizan el desarrollo de una cultura organizacional sólida. Además de la tercerización.

   1.2 ¿Qué iniciativas o acciones considera necesarias para fortalecer la cultura de gestión de riesgos en una organización y superar las limitaciones identificadas?

   Se considera que una de las acciones primordiales es poder integrar a toda la organización en la cultura de gestión de riesgos, promoviendo la participación activa de todas las áreas y niveles jerárquicos.

2. La encuesta identificó desafíos como la resistencia al cambio, débil cultura organizacional y la falta de estructuración en los procesos de gestión de riesgos.

   2.1 ¿De qué manera considera que estos factores se relacionan entre sí y cómo afectan el fortalecimiento de la gestión de riesgos en el área de TI?

   Se considera que factores como la resistencia al cambio, una cultura organizacional débil y la falta de estructuración en los procesos de gestión de riesgos están estrechamente relacionados, ya que se retroalimentan entre sí y dificultan la adopción de prácticas efectivas. Estos desafíos pueden derivar en consecuencias como el deterioro de la reputación institucional y la renuncia de personal clave, lo cual compromete la estabilidad y continuidad operativa de la organización.

2.2 En su ex experiencia, ¿Cuál de estos desafíos representa el mayor obstáculo para avanzar en la gestión de riesgos y por qué?

Se considera que la resistencia al cambio.

2.3 Además, ¿Qué acciones concretas, según su experiencia, han resultado efectivas para formalizar los procesos de gestión de riesgos?

Se considera que el establecimiento de una adecuada gobernanza de TI, la alineación de las iniciativas tecnológicas con los objetivos estratégicos del negocio y la realización periódica de auditorías externas son acciones efectivas. Estas acciones permiten fortalecer los controles, asegurar el cumplimiento normativo y garantizar una gestión de riesgos más estructurada y proactiva.

3. La encuesta evidencia que el 75% de las instituciones participantes aún no utilizan inteligencia artificial en sus procesos de gestión de riesgos. No obstante, el 25% que han explorado su implementación han enfrentado obstáculos como la complejidad técnica y la resistencia al cambio.

3.1 Desde su experiencia, ¿qué estrategias han sido más efectivas para gestionar la resistencia del personal frente a la incorporación de nuevas tecnologías?

Se considera que se debe tener una comunicación clara y oportuna sobre los beneficios y objetivos de las nuevas tecnologías. Además de las capacitaciones continúas enfocadas tanto en el uso de la herramienta como en la gestión de riesgos asociados. También se consideró importante la impartición de charlas que fomenten espacios para participación activa del personal y promuevan una cultura abierta al cambio.

3.2 Desde su perspectiva, ¿qué condiciones o factores considera necesarios para que una institución se sienta preparada para integrar soluciones basadas en IA en la gestión de riesgos?

Se considera que, para que una institución se sienta preparada para integrar soluciones basadas en inteligencia artificial en la gestión de riesgos, es fundamental implementar herramientas seguras. La falta de conocimiento sobre este tipo de tecnologías puede generar desconfianza y resistencia a su adopción, especialmente por el temor a posibles riesgos asociados a su uso.

4. La encuesta revela que COBIT 2019 e ITIL son marcos comúnmente utilizados para la gestión de riesgos en TI. **Desde su experiencia, ¿cómo ha aplicado los principios de estos marcos para identificar, evaluar o mitigar riesgos tecnológicos?**

Se han aplicado conforme a la información proporcionada por la Guía de Implementación de COBIT 2019.

5. El 50% de los encuestados perciben de manera neutral la colaboración entre la gestión de riesgos de TI y la auditoría interna. **Desde su experiencia, ¿cuáles acciones considera fundamentales para fortalecer la colaboración entre la gestión de riesgos de TI y la auditoría interna?**
   Se considera fundamental establecer una comunicación efectiva y continua entre ambas áreas. Además, es importante programar revisiones conjuntas periódicas, llevar a cabo evaluaciones integradas y realizar simulaciones de planes de continuidad, lo cual permite alinear criterios, identificar oportunidades de mejora y fortalecer la colaboración entre la gestión de riesgos de TI y la auditoría interna.

6. **¿Qué elementos y buenas prácticas considera esenciales para diseñar e implementar un sistema efectivo de gestión de riesgos en el área de tecnologías de la información?**
   Se considera fundamental contar con manuales actualizados que orienten los procesos de gestión de riesgos en tecnologías de la información. Asimismo, es esencial brindar capacitación continua al personal, de manera que se fortalezca la cultura organizacional en torno a la gestión de riesgos. Otra buena práctica es incorporar formalmente la gestión de TI dentro del marco de gobernanza corporativa, asegurando así su alineación con los objetivos estratégicos de la organización. Finalmente, disponer de una infraestructura tecnológica robusta y bien gestionada permite mitigar vulnerabilidades y responder eficazmente ante incidentes.

Anexo 2. Entrevista N.° 2: Profesional en gestión de riesgos en TI

Asunto	Entrevista enfocada en la gestión de riesgos en TI			**Responsable**	Ivannia Rojas Gutiérrez
Modalidad	Vía zoom	**Hora inicio**	08:00 am		
Fecha	07/08/2025	**Duración total**	20 minutos	**Entrevista N.°**	2

Resumen de hallazgos

1. Uno de los hallazgos obtenidos a partir de la encuesta aplicada en instituciones financieras de carácter local en Costa Rica indica que la cultura de gestión de riesgos en el área de tecnologías de la información (TI) es percibida como moderada por los encuestados.

   1.1 ¿Qué factores considera que limitan actualmente el desarrollo de una cultura sólida de gestión de riesgos en TI dentro una organización?

   La falta de alineación entre el área de TI y el negocio se reconoció como uno de los principales factores que dificultan el desarrollo de una cultura sólida de gestión de riesgos en TI.

   En muchas empresas, TI opera de manera aislada, sin una integración efectiva con los objetivos estratégicos ni con los procesos críticos del negocio. Esta separación provoca que los equipos de TI no siempre estén sensibilizados ni capacitados en temas de gestión de riesgos, enfocándose más en la operación técnica que en el impacto que los riesgos tecnológicos pueden tener sobre la continuidad del negocio o la reputación institucional.

   A pesar de que la SUGEF ha venido fortaleciendo este tema mediante la emisión de normativa específica, como la SUGEF 14-17, que establece los lineamientos para la gestión y control de las tecnologías de información en las entidades supervisadas, aún persiste una brecha importante en la capacitación y alineamiento de los equipos de TI con las necesidades de gestión de riesgos.

   1.2 ¿Qué iniciativas o acciones considera necesarias para fortalecer la cultura de gestión de riesgos en una organización y superar las limitaciones identificadas?

   Se consideró fundamental integrar a TI en la toma de decisiones estratégicas y asegurando que sus equipos comprendan los marcos regulatorios aplicables, así como la importancia de su rol en la protección de los activos de información y la continuidad operativa de la organización.

2. La encuesta identificó desafíos como la resistencia al cambio, débil cultura organizacional y la falta de estructuración en los procesos de gestión de riesgos.

   2.1 ¿De qué manera considera que estos factores se relacionan entre sí y cómo afectan el fortalecimiento de la gestión de riesgos en el área de TI?

Se consideró que la resistencia al cambio suele surgir cuando no existe una cultura organizacional sólida, y la falta de alineación con los objetivos estratégicos. Aunque existen procesos, su madurez es baja y no están totalmente integrados al negocio.

2.2 En su experiencia, ¿Cuál de estos desafíos representa el mayor obstáculo para avanzar en la gestión de riesgos y por qué?

Se consideró que el mayor obstáculo para avanzar en la gestión de riesgos es el limitado apoyo organizacional. Cuando la alta dirección no impulsa ni prioriza este tema, los esfuerzos desde otras áreas pierden fuerza, se carece de recursos. Esta falta de respaldo también se refleja en presupuestos reducidos para capacitación y en la ausencia de una alineación entre los objetivos estratégicos y la gestión de riesgos de TI. Sin un compromiso real desde los niveles superiores, difícilmente se consolida una cultura organizacional que valore y promueva la gestión proactiva del riesgo.

2.3 Además, ¿Qué acciones concretas, según su experiencia, han resultado efectivas para formalizar los procesos de gestión de riesgos?

Se consideró que una de las acciones que ha resultado para formalizar los procesos de gestión de riesgos es la participación activa del área responsable de riesgos (Gerente de riesgos o coordinador, jefatura) en la planificación estratégica institucional. Esto permite incorporar al menos un objetivo estratégico directamente alineado a la gestión de riesgos, lo cual no solo le da visibilidad y relevancia al tema, sino que también asegura el compromiso de la alta dirección y facilita la asignación de recursos

3. La encuesta evidencia que el 75% de las instituciones participantes aún no utilizan inteligencia artificial en sus procesos de gestión de riesgos. No obstante, el 25% que han explorado su implementación han enfrentado obstáculos como la complejidad técnica y la resistencia al cambio.

3.1 Desde su experiencia, ¿qué estrategias han sido más efectivas para gestionar la resistencia del personal frente a la incorporación de nuevas tecnologías?

No se brindó una respuesta, dado que el entrevistado no ha tenido experiencia con procesos de adopción tecnológica que generen resistencia por parte del personal.

3.2 Desde su perspectiva, ¿qué condiciones o factores considera necesarios para que una institución se sienta preparada para integrar soluciones basadas en IA en la gestión de riesgos?

Se consideró que contar con sistemas que permitan implementar herramientas de IA de forma segura y eficiente es uno de los factores que se consideran necesarios.

4. La encuesta revela que COBIT 2019 e ITIL son marcos comúnmente utilizados para la gestión de riesgos en TI. **Desde su experiencia, ¿cómo ha aplicado los principios de estos marcos para identificar, evaluar o mitigar riesgos tecnológicos?**

   Se reconoció que estos marcos son guías para adoptar buenas prácticas en la gestión de riesgos tecnológicos, ya que se ajustan a la naturaleza y necesidades específicas de cada empresa, lo que facilita su aplicación. Sin embargo, se destaca que estos marcos orientan sobre qué se debe hacer, pero no siempre explican cómo implementarlo en la práctica. Por ello, sin los recursos adecuados, especialmente en capacitación, la adopción efectiva de estos marcos puede verse limitada, afectando el verdadero fortalecimiento de la gestión de riesgos tecnológicos.

5. El 50% de los encuestados perciben de manera neutral la colaboración entre la gestión de riesgos de TI y la auditoría interna. **Desde su experiencia, ¿cuáles acciones considera fundamentales para fortalecer la colaboración entre la gestión de riesgos de TI y la auditoría interna?**

   Una de las acciones que se consideró fundamentales es contar con personal altamente calificado, especialmente con especialistas en auditoría de tecnologías de la información. Muchas veces, la ausencia de expertos en TI dentro del equipo de auditoría limita la capacidad para identificar oportunamente riesgos tecnológicos y formular recomendaciones efectivas que contribuyan a la mejora continua.

6. **¿Qué elementos y buenas prácticas considera esenciales para diseñar e implementar un sistema efectivo de gestión de riesgos en el área de tecnologías de la información?**

   Se consideró que los marcos de referencia son excelentes guías para adoptar buenas prácticas. Sin embargo, antes de considerarlos, es fundamental realizar un estudio técnico que permita evaluar la situación particular de la empresa. Esto facilita identificar cuáles prácticas son realmente aplicables y adecuadas a su contexto. Es importante tener en cuenta que la implementación de buenas prácticas con frecuencia implica un alto esfuerzo económico, lo que puede no ser rentable para algunas empresas para otras no. Así que en conclusión todo depende para la empresa en que se esté trabajando.

Anexo 3. Entrevista N.° 3: Profesional en gestión de riesgos en TI

Asunto	Entrevista enfocada en la gestión de riesgos en TI			**Responsable**	Ivannia Rojas Gutiérrez
Modalidad	Vía zoom	**Hora inicio**	5:00 pm		
Fecha	13/08/2025	**Duración total**	20 minutos	**Entrevista N.°**	3

Resumen de hallazgos

1. Uno de los hallazgos obtenidos a partir de la encuesta aplicada en instituciones financieras de carácter local en Costa Rica indica que la cultura de gestión de riesgos en el área de tecnologías de la información (TI) es percibida como moderada por los encuestados.

   1.1 ¿Qué factores considera que limitan actualmente el desarrollo de una cultura sólida de gestión de riesgos en TI dentro una organización?

   Se considera que las instituciones financieras de Costa Rica han crecido bastante por medio de las regulaciones en materia de Tecnologías de Información, se indica que las entidades financieras supervisadas de menor tamaño se les ha dificultado adaptar o adoptar mejores prácticas como el COBIT, ITIL, ISO 31000, ISO 27000, etc, se considera que el factor recursos ha limitado para estas entidades alinearse a los reglamentos a un mismo nivel que entidades de mayor solvencia y capacidad de invertir recursos de esta índole. Se ha notado una reducción en la cantidad de entidades financieras por diversos factores, algunas se han tenido que absorber por otras de mayor tamaño, se ha valorado una regulación proporcional que podría no ser la solución y también ha ocurrido que, aunque se tenga recursos la cultura no ha permeado de manera responsable.

   1.2 ¿Qué iniciativas o acciones considera necesarias para fortalecer la cultura de gestión de riesgos en una organización y superar las limitaciones identificadas?

   Se considera necesario que se identifique por parte de la alta administración el valor de adoptar y adaptar mejores prácticas, no sólo por un tema de cumplimiento hacia las superintendencias, sino para que forme parte de los procesos de las entidades incluyendo al proceso de Tecnologías de Información.

2. La encuesta identificó desafíos como la resistencia al cambio, débil cultura organizacional y la falta de estructuración en los procesos de gestión de riesgos.

   2.1 ¿De qué manera considera que estos factores se relacionan entre sí y cómo afectan el fortalecimiento de la gestión de riesgos en el área de TI?

Se considera que estos factores si están relacionados y debe venir desde la alta administración y ser parte de todos los procesos de la entidad, incluyendo a Tecnologías de Información.

2.2 En su experiencia, ¿Cuál de estos desafíos representa el mayor obstáculo para avanzar en la gestión de riesgos y por qué?

Se considera según el criterio del entrevistado que es un tema de cultura organizacional y debe definirse políticas y lineamientos claros desde la alta administración.

2.3 Además, ¿Qué acciones concretas, según su experiencia, han resultado efectivas para formalizar los procesos de gestión de riesgos?

Se considera que estos temas se deben conversar en los respectivos comités, consejos de administración o juntas directivas; se definan políticas y se evalúe el cumplimiento anualmente.

3. La encuesta evidencia que el 75% de las instituciones participantes aún no utilizan inteligencia artificial en sus procesos de gestión de riesgos. No obstante, el 25% que han explorado su implementación han enfrentado obstáculos como la complejidad técnica y la resistencia al cambio.

3.1 Desde su experiencia, ¿qué estrategias han sido más efectivas para gestionar la resistencia del personal frente a la incorporación de nuevas tecnologías?

Se considera que es importante que este tipo de iniciativas se definan como proyectos institucionales y que lleven respaldo de la alta administración.

3.2 Desde su perspectiva, ¿qué condiciones o factores considera necesarios para que una institución se sienta preparada para integrar soluciones basadas en IA en la gestión de riesgos?

Se considera primero definir políticas y lineamientos claros y que se definan proyectos formales con objetivos claros y alineado a las políticas o estrategia institucional.

4. La encuesta revela que COBIT 2019 e ITIL son marcos comúnmente utilizados para la gestión de riesgos en TI. **Desde su experiencia, ¿cómo ha aplicado los principios de estos marcos para identificar, evaluar o mitigar riesgos tecnológicos?**

Se indica que COBIT o ITIL definen aspectos generales, desde el criterio del entrevistado se considera que un marco más robusto es la ISO 31000 para crear un método institucional para gestionar los riesgos de la entidad, incluyendo los riesgos de Tecnologías de Información.

5. El 50% de los encuestados perciben de manera neutral la colaboración entre la gestión de riesgos de TI y la auditoría interna. **Desde su experiencia, ¿cuáles acciones considera fundamentales para fortalecer la colaboración entre la gestión de riesgos de TI y la auditoría interna?**

   Se considera que debe definirse claramente el rol de cada línea de defensa, desde una perspectiva de la generación de valor y considerando a Tecnologías de Información, TI debe crear el valor o generar beneficios como por ejemplo asegurar continuidad, seguridad de la información, eficientizar por medio de la tecnología los procesos de negocio; el área de riesgos debe conservar el valor o beneficios que genera TI y la auditoría interna mediante un criterio independiente debe asegurar la efectividad de la generación de valor de TI y de cómo riesgos conserva dicho valor.

6. **¿Qué elementos y buenas prácticas considera esenciales para diseñar e implementar un sistema efectivo de gestión de riesgos en el área de tecnologías de la información?**

   Se considera que se debe adoptar y adaptar mejores prácticas de la industria, como COBIT, ITIL, ISO 31000, TOGAF, ISO 27000, etc, este tipo de marcos deben ser analizados y revisados, para ser incorporados en la normativa según corresponda de cada entidad, según el apetito de riesgo, el volumen transaccional, complejidad, etc.

Anexo 4. Validación de criterio experto

Asunto	Validar la propuesta de solución			**Experto**	Norberto Lee Rodríguez Madrigal
Modalidad	Vía zoom	**Hora inicio**	8:30 am		
Fecha	12/11/2025	**Duración total**	45 minutos	**Puesto**	Gerente de TI

Resumen de recomendaciones
Se sugiere que, en la segunda dimensión (principio dos), se contemple la primera línea de defensa. Si bien ya se consideran la segunda y la tercera línea, sería conveniente reforzar la inclusión de la primera, dado que representa la línea principal de defensa en la gestión de riesgos. Como recomendación adicional, se sugiere incorporar la cuarta y quinta línea de defensa. 1. Primera línea: TI 2. Segunda línea: Gestión de riesgos 3. Tercera línea: Auditoría interna 4. Auditoría externa 5. SUGEF Adicionalmente, en relación con el principio 4, se sugiere incorporar herramientas que faciliten la comunicación y el acceso a la información entre todas las líneas de defensa, fortaleciendo así la coordinación y el flujo de información.
En relación con la dimensión 3, se sugiere reconocer que cada organización define su propia metodología para establecer el apetito de riesgo. En este sentido, la solución propuesta puede considerarse como una alternativa válida que podría apoyar dicho proceso.
Respecto a la cuarta dimensión: 1. Se sugiere aprovechar la IA como un recurso complementario para enriquecer la información del proceso de gestión de riesgos. No obstante, es importante reforzar que siempre debe mantenerse la validación y criterio humano para interpretar y confirmar los resultados generados por estos modelos. 2. Se recomienda asegurar la privacidad de los datos utilizados en los modelos de IA, considerando que la información empleada suele ser de carácter sensible, confidencial, restringida o de uso interno.

3. Se sugiere que las plataformas o arquitecturas de IA provistas por terceros deben asegurar la debida separación respecto a otros modelos públicos o privados, resguardando la privacidad e integridad de los modelos desarrollados por la organización.