Propuesta de implementación de una guía metodológica basado en RISK IT como estrategia para la gestión de riesgos con el fin de mejorar la eficiencia de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador - PUCE

Arcos Villagómez, Suyana Fabiola

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

MSc. Tapia León, Freddy Mauricio

9 de noviembre del 2021

Curiginal

Document Information

Analyzed document	Tesis total_V7_12-oct-2021.docx (D116892752)
Submitted	2021-10-30 02:44:00
Submitted by	Ramiro Delgado
Submitter email	pg.docenterdr@uniandes.edu.ec
Similarity	5%
Analysis address	pg.docenterdr.unia@analysis.urkund.com

FREDDY MAURICIO TAPIA LEON

Sources included in the report

SA	**TESIS_23_04_2018.docx** Document TESIS_23_04_2018.docx (D37887466)	2
SA	**MinchalaPablo_TesisFinal.docx** Document MinchalaPablo_TesisFinal.docx (D18372203)	6
SA	**ASI_V1.docx** Document ASI_V1.docx (D32782705)	5
SA	**TESIS FINAL.docx** Document TESIS FINAL.docx (D43785651)	17
SA	**Capitulo 1.docx** Document Capitulo 1.docx (D9759952)	2
SA	**revision enviar.docx** Document revision enviar.docx (D14020441)	7
SA	**Tesis-CGE v.2.3.docx** Document Tesis-CGE v.2.3.docx (D35625533)	7
SA	**TRABAJO DE TITULACION SAYDE OCHOA2.pdf** Document TRABAJO DE TITULACION SAYDE OCHOA2.pdf (D12787869)	15
SA	**Desarrollo de Tesis.docx** Document Desarrollo de Tesis.docx (D32490473)	3
SA	**MONOGRAFIA JOSELIN PACHECO - FINAL.docx** Document MONOGRAFIA JOSELIN PACHECO - FINAL.docx (D23868101)	2
SA	**1433451819_652__An%2525C3%2525A1lisis%2528de%2528sistemas%2528-%2529david.pptx** Document 1433451819_652__An%2525C3%2525A1lisis%2528de%2528sistemas%2528-%2529david.pptx (D14767637)	1
SA	**Tesis_Capitulo_I_II_HoldingDine.docx**	1

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"Propuesta de implementación de una guía metodológica basado en RISK IT como estrategia para la gestión de riesgos con el fin de mejorar la eficiencia de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador - PUCE"** fue realizado por la señorita ***Arcos Villagómez, Suyana Fabiola*** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 9 de noviembre del 2021

Firma:

FREDDY MAURICIO TAPIA LEON

Tapia León, Freddy Mauricio

Director

C.C.: 1714745690

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo, ***Arcos Villagómez, Suyana Fabiola,*** con cédula de ciudadanía n° 170585893-2, declaro que el contenido, ideas y criterios del trabajo de titulación: **Propuesta de implementación de una guía metodológica basado en RISK IT como estrategia para la gestión de riesgos con el fin de mejorar la eficiencia de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador - PUCE** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 9 de noviembre del 2021

Firma:

Suyana Arcos V.

.....

Arcos Villagómez, Suyana Fabiola

C.C.: 170585893-2

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo, ***Arcos Villagómez, Suyana Fabiola,*** con cédula de ciudadanía nº 170585893-2, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Propuesta de implementación de una guía metodológica basado en RISK IT como estrategia para la gestión de riesgos con el fin de mejorar la eficiencia de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador - PUCE** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 9 de noviembre del 2021

Firma:

Suyana Arcos V.

.....

Arcos Villagómez, Suyana Fabiola

C.C.: 170585893-2

DEDICATORIA

A mi familia: Patricia, Tamia y Leo.

Suyana Arcos Villagómez

AGRADECIMIENTO

Expreso mi agradecimiento a quienes facilitaron todos los procesos para que esta tesis se lleve a cabo. A los miembros de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador, en especial a Orlando Acosta y Fabián Negrete. A los responsables de la Dirección de Posgrados y Maestría en Gerencia de Sistemas de la Universidad de las Fuerzas Armadas ESPE. Al director del presente trabajo de titulación Freddy Tapia por su guía y acompañamiento. A la motivación y generosa amistad de Gabriela Fernández y Gustavo Chafla.

Suyana Arcos Villagómez

INDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El riesgo es la combinación de la probabilidad de que ocurra un evento riesgoso y además el resultado del mismo cuando sucede. Tiene influencia sobre los objetivos que se ha planteado la organización porque puede desviarlos de lo planificado hacia positivo o hacia negativo. El riesgo, pero también las oportunidades conviven y la gestión de ambos es una actividad estratégica clave para el éxito de la organización. Entonces, la gestión de riesgos es el proceso de identificar y aplicar medidas de control para contrarrestar los eventos riesgosos y por consiguiente proteger los activos de la organización mediante actividades aprobadas y coordinadas que lleven a la empresa a cumplir las metas propuestas. La presente tesis propone una guía para la gestión de riesgos basada en la herramienta RISK IT de ISACA, herramienta aplicada a nivel global. Para cumplir con el propósito se decidió, en primera instancia, una ruta de investigación mixta que permitió enfocar la investigación. En segundo lugar, se documentó el desarrollo del componente técnico para la presente tesis; desarrollándose una metodología específica, basada en RISK IT, para el caso de estudio sobre los activos de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador (PUCE). Dentro de la guía metodológica propuesta constan los ámbitos de Gobernar el Riesgo, Evaluar el Riesgo y Responder al Riesgo y nueve procesos que van desde gobernar el riesgo, administrarlo, recopilar datos, analizar riesgos, responder a los riesgos mediante controles y recomendar estrategias para comunicarlos y expresarlos de modo que la gestión de riesgos se convierta en parte de la cultura de riesgos organizacionales.

- Palabras Clave:

- **GOBERNAR EL RIESGO**
- **EVALUAR EL RIESGO**
- **RESPONDER AL RIESGO**
- **GESTIÓN DE RIESGOS DE TI**

ABSTRACT

Risk is the combination of the probability that a risky event will occur and also the result of it when it happens. It influences the objectives that the organization has set for itself because it can deviate them from what is planned towards positive or negative. Risk, but also opportunities coexist and the management of both is a key strategic activity for the success of the organization. Then, risk management is the process of identifying and applying control measures to counteract risky events and therefore protect the assets of the organization through approved and coordinated activities that lead the company to meet the proposed goals. This thesis proposes a guide for risk management based on ISACA's RISK IT tool, a tool applied globally. To fulfill the purpose, a mixed research route was decided, in the first instance, that allowed the research to be focused. Second, the development of the technical component for this thesis was documented; developing a specific methodology, based on RISK IT, for the case study on the assets of the Information Technology Directorate of the Pontificia Universidad Católica del Ecuador (PUCE). The proposed methodological guide includes the areas of Governing Risk, Assessing Risk and Responding to Risk and nine processes that range from governing risk, managing it, collecting data, analyzing risks, responding to risks through controls and recommending strategies to communicate them and express them so that risk management becomes part of the organizational risk culture.

- Keywords:

- **GOVERN RISK**
- **ASSESS RISK**
- **RESPOND TO RISK**
- **IT RISK MANAGEMENT**

CAPÍTULO I

Generalidades

Antecedentes

Existen varias definiciones relacionadas al tema de Gestión de Riesgos, a continuación, se escriben las más destacadas:

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

La Dirección de Informática de la PUCE es una unidad encargada de la conectividad, servicios tecnológicos, accesibilidad a la red, soporte técnico, soporte académico y desarrollo de aplicaciones, etc. Además, al poseer infraestructura de TI, se realizan actividades para el desenvolvimiento diario de la entidad de educación superior en el ámbito de la informática, actividades que son expuestas hacia amenazas internas o externas. Un tema como el propuesto en el presente trabajo de titulación, plantea desarrollar una guía metodológica, el cual servirá de guía para esta dirección, misma que se propone en términos de mejoramiento y optimización asociada a las funciones anteriormente descritas. A pesar de que, existen estándares para gestionar riesgos, como el proceso desarrollado por la ISO 31000 (ISO, 2019). También existen marcos metodológicos como RISK IT que se diferencia de otros modelos de riesgos, debido a que mientras la mayoría de aquellos, busca eliminar los riesgos, RISK IT “considera la posibilidad de ir en la búsqueda de riesgos que, bien gestionados, podrían beneficiar a

la organización, siempre que se encuentre el balance adecuado entre riesgo y valor" (ISACA, 2020, pág. 7).

La Dirección de Informática, al poseer infraestructura de tecnologías de información, realiza diferentes actividades, las cuales se relacionan con su función, lo que permite su exposición y enfrentamiento a diversos riesgos asociados. Es por estas razones que el presente trabajo de titulación pretende aportar y coadyuvar a la labor que viene desarrollando esta dirección.

Cabe indicar que se aplicó un cuestionario al Director de Informática de la PUCE, con aquel, se verificó que la gestión de riesgos se realiza de forma parcial, lo cual motivó a realizar un aporte que incentive una planificación, gestión y tratamiento de los riesgos.

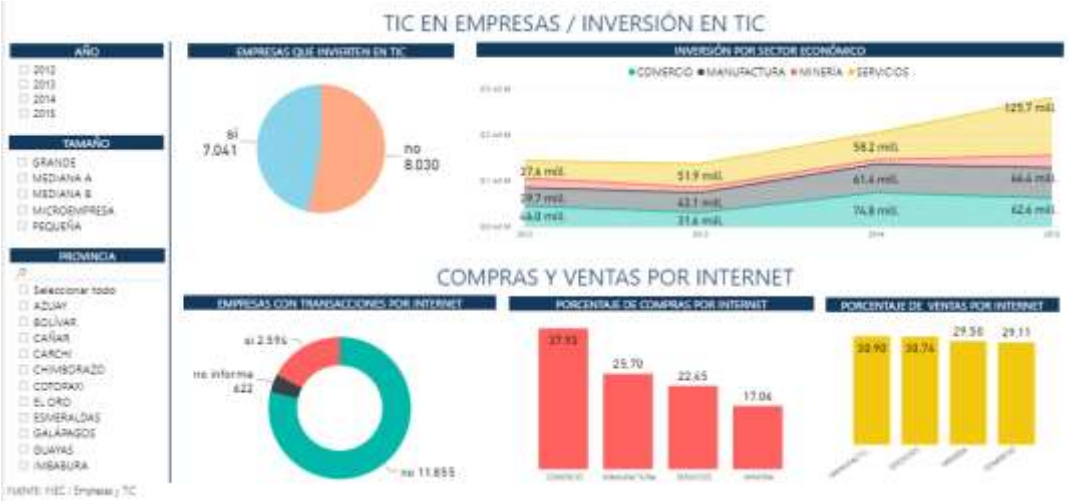
Planteamiento del Problema

El acceso a las Tecnologías de la Información y Comunicación constituye un derecho de todos los ciudadanos. Por ello, a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información, se promueve el desarrollo de la sociedad con servicios tecnológicos modernos, por medio del acceso al Internet, dotación de equipamiento y capacitación a niños, jóvenes y adultos del Ecuador (MINTEL, 2019).

En la figura 1, se muestra con cifras que, en los últimos tres años, Ecuador aumentó su inversión en TIC de 37,6 millones a 125,7 millones en tres años, de 2012 a 2015.

Figura 1.

Estadísticas de Inversión en TIC



Tomado de: (MINTEL, 2019)

Por lo tanto, se esperaría que cuando existe mayor inversión en tecnologías mayores serían las actividades derivadas de la misma (Jaramillo, 2013). Entre estas actividades estarían, las labores de seguimiento, control y evaluación de TI y más aún la tendencia actual derivada de estas, que es la gestión de riesgos: identificar, gobernar y administrar los mismos.

De la revisión de la literatura y de los estudios previos realizados, sobre la temática de gestión de riesgos, a nivel local, se encontró que:

- En empresas públicas y privadas, en las áreas de TI, se evidencia que la calificación de la gestión de riesgos de TI es moderada. Destacan las entidades privadas teniendo una gestión buena pero no, excelente (Jaramillo, 2013).
- Así mismo, en empresas públicas y privadas, se demuestra que los encargados de las áreas de TI conocen de los peligros sobre sus sistemas informáticos, destacan las organizaciones privadas donde se tiene un alto conocimiento sobre

el tema y es más elevado que en las entidades públicas, cuyo porcentaje de conocimiento es moderado (Jaramillo, 2013).

- Además, en empresas públicas y privadas, se determina que las áreas de TI conocen sobre el impacto del riesgo de pérdida de información, organizaciones privadas tienen un mayor porcentaje que las empresas públicas sobre el tema (Jaramillo, 2013).

Así mismo, analizando más específicamente, se aplicó un cuestionario al Director de Informática de la PUCE, dentro de las preguntas realizadas consta:

- Si se cuenta con indicadores de desempeño que permitan evaluar el funcionamiento de los sistemas informáticos e infraestructura de TI.
- Si se cuenta con un plan sistémico para gestionar los riesgos sobre los sistemas informáticos e infraestructura de TI.
- Si se ha instruido al personal de informática para que conozca los riesgos de TI.
- Si se ha tenido limitaciones técnicas y económicas para implementar un plan sistémico para gestionar riesgos.
- Si la Dirección de Informática tiene medido el impacto que implicaría una fuerte debilidad de vulneración de los sistemas informáticos e infraestructura de TI.

Del análisis, se identificó que la gestión de riesgos en la Dirección de Informática de la universidad se realiza parcialmente. Encontrando en este factor una posibilidad para la realización de una propuesta que abarque la gestión de riesgos de la misma mediante el uso de herramientas utilizadas en las empresas a nivel global como son COBIT 5 y RISK IT. COBIT 5 es un marco de negocios creado para gobernar y gestionar las TI en las organizaciones y RISK IT fue desarrollado para apoyar la gestión de riesgos relacionados con TI

Objetivo General

Desarrollar una propuesta de implementación de una guía metodológica (marco de referencia para seguir las mejores prácticas en cuanto a procesos, servicios y recursos) basado en RISK IT como estrategia para la gestión de riesgos con el fin de mejorar la eficiencia de la Dirección de Informática de la PUCE.

Objetivos Específicos

- Investigar sobre el estado del arte asociado a la gestión de riesgos por medio de una revisión literaria sobre marcos metodológicos o marcos de referencia, gestión de riesgos y gestión de riesgos basado en COBIT 5 y RISK IT.
- Determinar los aspectos relevantes de la Gestión de Riesgos basados en la herramienta RISK IT de COBIT 5 como punto de partida en el tratamiento de los mismos para aplicar este conocimiento al estudio de caso particular de la Dirección de Informática de la PUCE.
- Identificar y evaluar la situación actual de la Dirección de Informática de la PUCE mediante un levantamiento de la información relacionada con la gestión de riesgos por cada una de las áreas que la conforman para realizar un mapeo de la situación actual.
- Desarrollar una propuesta de implementación de una guía metodológica basado en la herramienta RISK IT que se utilice para gestionar riesgos en la Dirección de Informática de la PUCE, por medio del análisis y la valoración de los hallazgos encontrados y que esto permita mejorar la eficiencia de la mencionada dirección.
- Evaluar la propuesta con la respectiva estimación de riesgos de TI, perfil de riesgos, respuesta al riesgo y el análisis integral de los mapas de riesgos sobre los recursos humanos, el hardware, el software, procesos internos y externos,

seguridad con la finalidad de verificar el mejoramiento en la eficiencia de la labor de la Dirección de Informática.

Justificación, Importancia y Alcance

Como se ha evidenciado anteriormente, son varios los aspectos que viabilizan y determinan la importancia de la presente investigación, más aún cuando la PUCE no cuenta con trabajos previos que sirvan de guía o soporte ante la gestión de riesgos por medio de un marco metodológico basado en estándares y buenas prácticas. Para esto se evaluará el impacto de implementar una gestión de riesgos mediante un modelo desarrollado y probado específicamente para el efecto, como lo es RISK IT de ISACA. Esta propuesta tiene el propósito de mejorar la eficiencia de la Dirección de Informática y podría ser replicada para otras instituciones de educación superior.

En cuanto al alcance, el trabajo de titulación culminará con la entrega de un documento de propuesta de implementación de una guía metodológica basado en RISK IT para la Dirección de Informática de la PUCE, documento que, de ser aplicado, permitirá identificar y tener conocimiento sobre los peligros e incidentes que surgen a partir de las acciones empresariales, mismos que pueden tener un efecto tanto negativo como positivo en el éxito de toda organización.

CAPÍTULO II

Gestión de Riesgos

Antecedentes Históricos

Antiguamente, se tenía una noción del riesgo relacionado con informática después de verificar que los resultados no eran los esperados o los que se habían planificado. Es decir, cuando faltaba el tiempo o el presupuesto en la ejecución de un proyecto, cuando fallaba el factor humano, cuando no funcionaba de manera eficiente el hardware o el software o cuando la seguridad informática había presentado deficiencias. En ese entonces, lo primero que se realizaba por parte del especialista encargado era buscar el origen o la fuente del riesgo, y aunque esta identificación constituía un avance, no resolvía el problema porque se conocía poco sobre la teoría de gestión de riesgos. Por lo tanto, el siguiente paso fue analizar los riesgos, es decir, a más de conocer su origen, se consideraba analizar la magnitud del daño causado o el costo en el caso de que llegara a ocurrir un incidente (Baca Urbina, 2016).

Consecuentemente, se observó que existían diferentes magnitudes de riesgos; más específicamente, se observó que existen riesgos que suceden pero afectan de manera poco perceptible; o también, existían riesgos que ocurrían y podían desviar un proyecto de su concepción original; así mismo, existían riesgos que al ocurrir ocasionaban ingentes costos en el momento en que se requería reparar el daño y también existían riesgos latentes pero con poca probabilidad de ocurrir; además, coexistían otros riesgos frecuentes pero resultaban ser inocuos (Baca Urbina, 2016).

Cuando se planifica sobre los riesgos, esta planificación no consiste solamente en identificar vulnerabilidades, medir el impacto y disminuir el riesgo de que sucedan, sino que se debe considerar el costo y algunas veces modificar el grupo de profesionales que trabajará relacionado a un proyecto, o cambiar un sistema,

infraestructura o tecnología. Sin embargo, por lo anotado anteriormente, la identificación del riesgo, el análisis y la mitigación de los efectos al ocurrir un riesgo, constituyen una base para la llamada gestión o administración de riesgos. Es de esperarse que con el paso del tiempo y la experiencia adquirida con la ejecución de proyectos de seguridad informática se haya ido más allá de las etapas que son la base en gestión de riesgos como son identificación, análisis y medidas para evitar los efectos de los riesgos. Actualmente, con el conocimiento que se acumuló sobre riesgos se gestiona de manera más apropiada los mismos (Baca Urbina, 2016).

Por consiguiente, en la temática de riesgos ha existido una evolución desde sus inicios en donde se tenía una noción limitada sobre estos temas. Se decidió analizar los riesgos; su origen y sus causas, la magnitud de los daños ocasionados y los recursos asociados. Consecuentemente, son clasificados dándose paso a una planificación o administración de riesgos hasta poder identificar su adecuado tratamiento.

Seguridad de la Información

La norma ISO 27001:2013 está alineada bajo la estructura de concepto de Sistema de Gestión de Seguridad de la Información. La cual establece una implementación efectiva de la seguridad de la información empresarial y considera como eje central la evaluación de riesgos.

La especificación de la Norma ISO 27001 (2013) indica que la seguridad consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como los sistemas implicados en el tratamiento de la misma dentro de la organización.

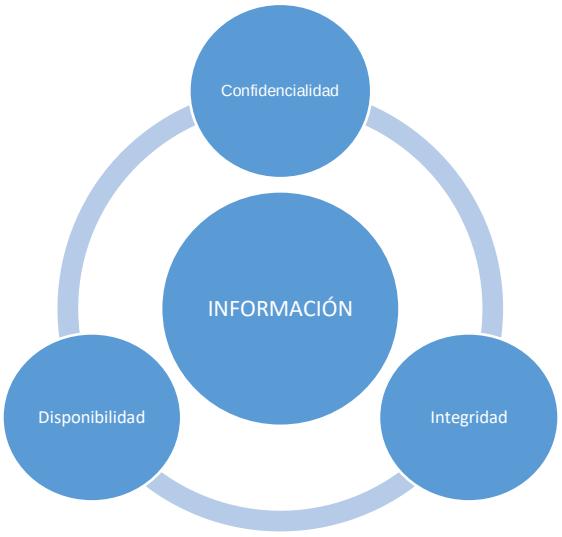
Términos que según la investigación de Valencia (2015) conforman la triada de la seguridad de la información[1], de la siguiente manera:

[1] La triada de la seguridad de la información hace referencia a la confidencialidad, integridad y autenticidad que representan los principios básicos de la triada de seguridad de la información según la International Organization for Standardization.

- Confidencialidad: Es un término asociado con el acceso y el uso de la información por parte de personas autorizadas. Es la propiedad de la información de no estar disponible o revelada ante los individuos, entidades o procesos que no hayan sido autorizados.
- Integridad: En términos generales podría definirse como la propiedad de salvaguardar la exactitud de la información y activos tecnológicos ante posibles modificaciones o destrucción. En términos específicos, de acuerdo con COBIT 5[2] la integridad está relacionada con la precisión, la completitud y la validez de la información.
- Disponibilidad: Es pertinente a que los usuarios autorizados tienen acceso a la información y activos tecnológicos cuando lo requieran. La Norma ISO 27001 la define como la propiedad de ser accesible y utilizable a petición de una entidad autorizada. Lo que se puede apreciar en la figura 2.

Figura 2.

Triada de la Seguridad de la Información



Tomado de: (Valencia, 2015)

[2] COBIT 5 fue creado por ISACA (proveedor de certificaciones, promoción y educación sobre seguridad, gobierno y gestión de TI). COBIT 5 contiene un marco de trabajo integral para gobierno y gestión de las TI corporativas.

Vulnerabilidades, Amenazas, Ataques e Impacto

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

La seguridad es la protección brindada a un sistema de información automatizado para alcanzar los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información esto incluye hardware, software, firmware, información, datos y telecomunicaciones (NIST, 2018). Al respecto la NIST[3] desarrolló un documento llamado Cybersecurity Framework (CSF) donde se brindan un conjunto de enfoques para reducir riesgos en infraestructura crítica; a través, de cinco pilares principales para administrar el riesgo como son identificar, proteger, detectar, responder y recuperar (OEA, 2019).

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

Una amenaza también es un estado o condición del entorno de los sistemas, áreas, dispositivos o infraestructura tecnológica que contienen información importante para una empresa u organización y que ante determinada situación podría producirse una violación en la seguridad y como efecto se afectaría la totalidad o parte de esa información.

[3] NIST, National Institute of Standards and Technology, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en normas y tecnología.

Cuando se determina que una amenaza podría perjudicar un activo se debe estimar la vulnerabilidad de dicho activo en cuanto a su degradación y en cuanto a su frecuencia. La degradación es el dimensionamiento del grado de perjuicio que sufriría un activo y la frecuencia está relacionada a la periodicidad de la ocurrencia de la amenaza. Se es vulnerable en la medida en que se carezca de protección suficiente para evitar que la amenaza llegue a ocurrir (Baca Urbina, 2016).

Un ataque es una amenaza que se lleva a ejecución tomando provecho de las vulnerabilidades y puede ser de naturaleza intencionada tal como ataques lógicos a los sistemas de información con propósito destructivo y puede tomar forma de vandalismo; o pueden existir ataques de naturaleza no intencionada como un incendio accidental, una inundación por condiciones del clima, etc. Una vulnerabilidad puede ser de todo tipo pero se debe cuantificar las vulnerabilidades que implican un riesgo mayor para crear planes adecuados (Erreyes, 2017).

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

Finalmente, el Instituto Nacional de Ciberseguridad de España (INCIBE), indica que la forma de medir el nivel de riesgo es una estimación de lo que puede ocurrir y se valora de forma cuantitativa, como la consecuencia del impacto asociado a una amenaza por la probabilidad de ocurrencia de la misma, como se indica en la figura 3:

Figura 3.

Cálculo del Riesgo

Tomado de: (Instituto Nacional de Ciberseguridad, 2017)

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

Riesgos

La Real Academia Española (2020) en su diccionario de la lengua española, describe al riesgo operativo como el riesgo que sufre una empresa derivado de la posibilidad de fallos en su propio funcionamiento.

En su concepción general, un riesgo tiene que ver con la probabilidad de que una amenaza se vuelva realidad. En cambio, en su concepción más específica se ha escogido las siguientes definiciones de riesgo como relevantes:

- La ISO 31000 (2018) refiere al riesgo como el efecto de la incertidumbre sobre los objetivos pudiendo ser positivo, negativo o ambos, y puede abordar, crear o generar oportunidades y amenazas. El riesgo generalmente se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y su probabilidad.

- La ISO 27005 (2011) define al riesgo como el potencial que tiene una determinada amenaza para explotar las vulnerabilidades de un activo y por consiguiente causar daño a una organización. El riesgo está relacionado con el uso y la adopción de las tecnologías de la información en una empresa u organización.
- La International Organization for Standarization, ISO (2014) define al riesgo como la combinación de la probabilidad de un evento y su consecuencia. Es la oportunidad de que algo ocurra y que tendrá impacto sobre los objetivos. Se mide en términos de consecuencia y posibilidad.
- Desde la perspectiva de la gestión de riesgos se define al riesgo como “la distribución de posibles desviaciones de los resultados esperados y de los objetivos; aquellos sucesos causados por eventos de incertidumbre, que podrían ser internos o externos a la organización” (Cienfuegos, 2013, pág. 21).
- El riesgo de origen tecnológico incide sobre las metas y objetivos de la organización. Por ello el daño, la interrupción, alteración o falla del uso de tecnologías de la información puede implicar pérdidas significativas en las organizaciones, además de pérdidas financieras, multas o acciones legales, además que se afecta la imagen de la organización y se causan inconvenientes a nivel operativo y estratégico (Ramirez & Ortiz, 2011).

Por lo tanto, el riesgo es la combinación de la probabilidad de que ocurra un evento y además el resultado cuando sucede. Tiene influencia sobre los objetivos que se ha planteado la organización porque puede desviarlos de lo planificado hacia positivo o hacia negativo. En el quinto capítulo del presente trabajo de titulación se identificarán los riesgos a los que está expuesta la Dirección de Informática de la PUCE que es el caso de estudio del presente trabajo de titulación.

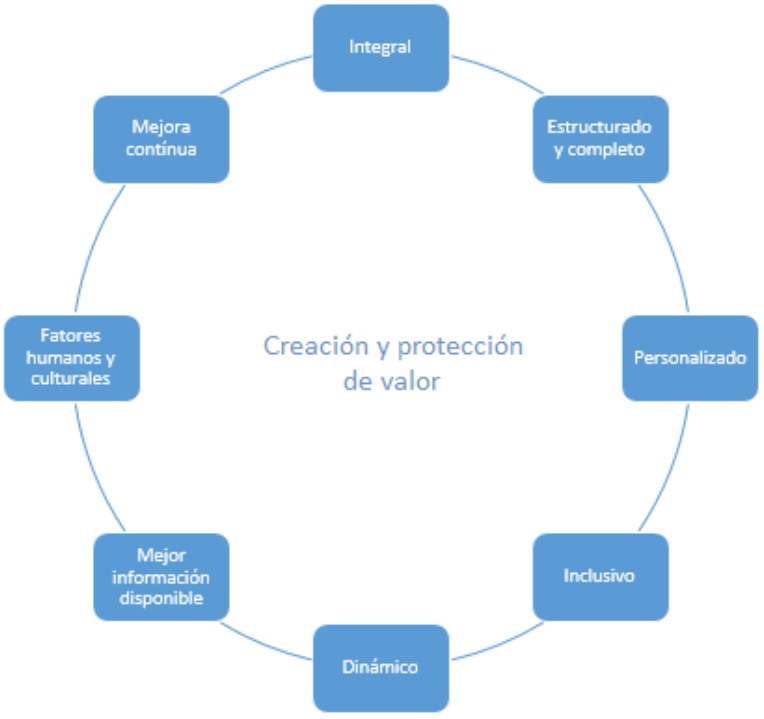
Principios de la Gestión de Riesgos

El propósito de la gestión de riesgos es la creación y protección de valor. Además de mejorar el rendimiento, fomentar la innovación y apoyar la consecución de objetivos de la empresa u organización (ISACA, 2020).

Los principios que se describirán en la figura 4, brindan orientación sobre las características de una gestión de riesgos eficaz y eficiente, comunicando su valor y explicando su intención y propósito. Los principios son la base y el punto de partida para la gestión de riesgos y deben tenerse en cuenta al establecer el marco de trabajo y los procesos de gestión de riesgos de la organización. Estos principios deberían permitir a una organización gestionar los efectos de la incertidumbre sobre sus objetivos (ISO, 2018).

Figura 4.

Principios de la Gestión de Riesgos



Tomado de: (ISO, 2018)

En el centro de la Figura 4 se muestra el propósito de la gestión de riesgos que es la creación y protección de valor. Alrededor, los principios de la gestión de riesgos que se explican a continuación:

- La gestión de riesgos es una parte integral de las actividades organizativas.
- Un enfoque estructurado e integral de la gestión de riesgos contribuye a resultados consistentes.
- El marco y el proceso de gestión de riesgos es personalizado y proporcional al contexto externo e interno de la organización relacionado con sus objetivos.
- La participación adecuada y oportuna de las partes interesadas permite considerar sus conocimientos, opiniones y percepciones, lo que da como resultado una mejor conciencia y una gestión de riesgos informada.
- Los riesgos pueden surgir, cambiar o desaparecer a medida que cambia el contexto interno y externo de una organización, la gestión de riesgos se anticipa, detecta, reconoce y responde a esos cambios y eventos de manera adecuada y oportuna.
- Los insumos para la gestión de riesgos se basan en información histórica y actual, así como en expectativas futuras. La gestión de riesgos tiene en cuenta las limitaciones e incertidumbres asociadas con dicha información y expectativas. La información debe ser oportuna, clara y estar disponible para las partes interesadas.
- El comportamiento humano y la cultura influyen significativamente en todos los aspectos de la gestión de riesgos en cada nivel y etapa.
- La gestión de riesgos se mejora continuamente mediante el aprendizaje y la experiencia (ISO, 2018).

Administración y Gestión del Riesgo

En la obra del autor (Baca Urbina, 2016), se indica que administrar es utilizar los recursos disponibles en la empresa para planificar acciones que ayuden a conseguir los objetivos planteados. En tal sentido, se pueden administrar el dinero, los recursos humanos o las propias instalaciones de la empresa. Incluye los mecanismos, acciones y formas a partir de las cuales se usan los recursos financieros, humanos y materiales de una compañía.

Gestionar, por su parte, es poner en marcha lo planificado durante la administración. Se puede gestionar un proceso de innovación, un plan de marketing, un sistema estandarizado para los departamentos de una empresa, etc.

La gestión empresarial alude a la planificación de los procesos para alcanzar los objetivos de una empresa u organización.

Realizadas estas diferenciaciones entre administración y gestión de riesgos se revisaron los planteamientos de algunos autores sobre cada temática y se muestran de la siguiente manera (Baca Urbina, 2016):

Sobre Administrar el Riesgo

La administración del riesgo considera que si un potencial riesgo se identifica desde el inicio este será menos costoso para la empresa u organización y hará menor daño. Siendo más conveniente ser proactivos que correctivos.

Para el autor Baca Urbina la administración del riesgo se divide en tres etapas:

1. Identificar y analizar o caracterizar el riesgo.
2. Definir una estrategia para administrar el riesgo.
3. Implementar planes de mitigación de efectos adversos cuando sea necesario.

A nivel general, la primera etapa comprende identificar la magnitud, probabilidad de ocurrencia y grado de afectación en caso de ocurrir un riesgo; en la segunda etapa se contemplan diferentes técnicas de mitigación como por ejemplo la simulación o los diseños alternativos de procesos de la empresa, y además los métodos y herramientas a utilizar para realizar las estrategias en caso de que el riesgo realmente ocurra. Finalmente, en la tercera etapa, que comprende un plan de mitigación, se debe declarar un límite mínimo y máximo que debe tomar el riesgo para empezar a actuar con el fin de regresar la situación bajo control (Baca Urbina, 2016).

A manera de complemento, el autor Estupiñán Gaitán (2006) afirma que la administración de riesgos empresariales (ERM[4]) es un proceso estructurado, consistente y continuo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos.

Para poder hablar de riesgos corporativos[5] (o del negocio) es importante contar con:

- Un buen sistema de control.
- Objetivos claramente definidos a nivel de estrategias, del mercado, de la tecnología, del recurso humano, de los procesos.
- Una auditoría basada en riesgos.
- Auditores líderes.
- Metodologías para auditar los riesgos.
- Metodologías corporativas de gestión de riesgos.

[4] Enterprise Risk Management, ERM, es una metodología que describe el conjunto de actividades que las empresas deben realizar frente al riesgo que enfrentan. Es un proceso sistemático para la identificación y evaluación de eventos o posibles riesgos y oportunidades.

[5] Riesgo corporativo está asociado con el uso, propiedad, operación, participación y adopción de las TI en una organización. Se compone de eventos negativos relacionados con las TI que potencialmente podrían afectar el negocio y que suponen dificultades para alcanzar las metas y objetivos estratégicos.

- Experiencia empresarial o corporativa con el manejo de los riesgos.
- Responsables sobre la gestión de riesgos.

Para que se puedan generar metodologías para administrar los riesgos es necesario haberlas asimilado con anterioridad, es decir, trabajar el riesgo como labor cotidiana porque forma parte del proceso metodológico. Una de las ventajas de trabajar la administración en base a situaciones de riesgos es que posteriormente sirven para la construcción de mapas de riesgo con los auditados (Estupiñán Gaitán, 2006).

Así también, una estructura conceptual común para administración de riesgos empresariales es COSO E.R.M.[6] que trata con riesgos y oportunidades que afectan la creación o preservación de valor. Está diseñado para identificar eventos potenciales que pueden afectar una organización y además para gestionar o administrar los riesgos a fin de proveer seguridad razonable en pos del logro de los objetivos de la entidad.

La administración de riesgos empresariales comprende (ISACA, 2020):

- Alinear el apetito por el riesgo con la estrategia: Cuando se evalúan las estrategias, se debe definir los objetivos relacionados y desarrollar los mecanismos para administrar los riesgos congruentes.
- Enriquecer o ampliar las decisiones de respuesta al riesgo: La administración de riesgos empresarial (ERM) provee el rigor para identificar y seleccionar entre las diferentes alternativas de respuesta al riesgo como evitarlo, reducirlo, compartirlo o aceptarlo.
- Minimizar sorpresas y pérdidas operacionales: Es inherente al ERM, que las entidades consigan capacidad para identificar eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costos o pérdidas asociados con estas.

[6] COSO, Committee of Sponsoring Organizations of the Treadway, estudia los factores y brinda recomendaciones sobre gestión de riesgo empresarial (ERM), control interno y disuasión al fraude.

- Identificar y administrar riesgos a lo largo de toda la organización y a los riesgos múltiples: Cada riesgo afecta a diferentes partes de la administración, el ERM facilita una respuesta efectiva a los impactos relacionados, así como respuestas integradas si los riesgos fueran múltiples.
- Sopesar oportunidades y adquirir ventaja: Mediante la consideración de un rango pleno de potenciales eventos, con el ERM la administración está posicionada para identificar y aprovechar de manera proactiva las oportunidades.
- Mejorar el despliegue y distribución del capital: La obtención de información robusta sobre riesgos le permite a la administración valorar de manera efectiva las necesidades, distribución y asignación de capital.

Las capacidades que provee la administración de riesgos empresariales (ERM), citadas anteriormente, le ayudan a la empresa a lograr los indicadores de desempeño y rentabilidad, así como a prevenir la pérdida de recursos. Además, que favorecen a asegurar el cumplimiento de leyes y regulaciones (Estupiñán Gaitán, 2006).

Mientras que, en la investigación de Ramírez y Ortiz (2011) se establece otra manera de administración de riesgos con enfoque en la mejora continua y en base a los estándares internacionales ISO 31000 e ISO 27005, con el esquema que se muestra a continuación:

- Planificar: Se establecen los objetivos y procedimientos para la gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes a las políticas y objetivos globales de la organización. Debería acompañarse de un plan de comunicación y un análisis del contexto organizacional con el objetivo de definir un alcance de la gestión de riesgos tecnológicos.

- Hacer: Concierne a la implementación de los controles, procedimientos e implementación de las políticas definidas. Corresponde a la valoración y tratamiento de los riesgos.
- Verificar: Realiza la evaluación y medición del desempeño de los procesos acorde a la política y los objetivos de seguridad de la organización y además informa sobre los resultados.
- Actuar: Establece una política para la gestión de riesgos tecnológicos e implementa los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar se incluye el monitoreo y mejora continua, donde se verifican los cambios y el cumplimiento de los indicadores determinados en la planificación.

Sobre Gestionar el Riesgo

"La gestión de riesgos incluye todas las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo" (ISO, 2018, pág. 1).

Así también, "La gestión de riesgos es el proceso de identificar y aplicar medidas de control para contrarrestar las amenazas basándose en el valor de los activos protegidos y en una evaluación de riesgo" (Ávalos, 2007, pág. 23).

> La gestión de riesgos es un proceso simultáneamente distribuido y centralizado, los expertos en cada parte de la empresa identifican y evalúan el riesgo en sus áreas, estos gerentes de riesgos locales abordan cada riesgo que controlan y escalan grandes riesgos a los gerentes con mayor autoridad. Los procesos promueven una vista global de todos los riesgos en un dominio, así los administradores pueden hacer compensaciones y priorizar el límite de recursos para formar un aceptable perfil de riesgos. (Westerman, 2006, pág. 23).

En condiciones ideales, la gestión de riesgos se debe efectuar por el departamento creado para el efecto, es decir el departamento de riesgos de la empresa u organización, pero es responsabilidad de todo el personal de la entidad y sus directivos. El departamento de gestión de riesgos debe encargarse de identificar eventos potenciales, gestionar los mismos dentro de lo aceptable y proporcionar seguridad a la organización. Entre las estrategias más comunes se incluyen la transferencia del riesgo, la evasión del riesgo, la reducción del efecto del riesgo ocurrido o la aceptación del riesgo y sus consecuencias. De tal forma de conseguir que las empresas sean capaces de absorber las perturbaciones sin alterar significativamente su estructura y funcionalidad, pudiendo regresar a su estado original una vez que la perturbación ha terminado y garantizando la continuidad del negocio (Martín Romeral & Torres Gallego, 2016).

Adicionalmente, según señala el autor Valencia (2015) existen etapas comunes en el proceso de gestión de riesgos desde el aspecto metodológico y se resumen en:

- Establecimiento del contexto.
- Identificación de riesgos.
- Análisis de riesgos.
- Evaluación o valoración de riesgos.
- Plan de tratamiento de riesgos.
- Monitoreo de riesgos.

Los riesgos se pueden dar sobre dos tipos de recursos: la información y los activos tecnológicos, sin embargo, frente a la evolución de la función de tecnologías de información, ha surgido el denominado servicio de TIC, como concepto integrador de recursos y cuyo origen se da al pasar de una gestión de recursos tecnológicos a una gestión de servicios de tecnologías de información. (Valencia, 2015, pág. 71).

El autor Chambi (2018) y las autoras Ramírez y Ortiz (2011) en sus investigaciones explican los criterios antes anotados:

- Establecimiento del Contexto: Es la definición de parámetros internos y externos a tomarse como base en la gestión de riesgos y el establecimiento del ámbito de aplicación para la política de gestión del riesgo. El contexto externo incluye el ámbito nacional, regional, jurídico, reglamentario, cultural, político, económico, tecnológico y la competencia. Interactúa con el ambiente interno incluye la estructura organizativa, responsabilidades y roles, misión, visión, las políticas y estrategias, los objetivos, las metas, los recursos, los sistemas de información, la cultura organizacional y normatividad interna. La importancia de tener claramente definidos estos aspectos es que se puede saber qué debe ser protegido y cuáles son las limitaciones para ejercer esta protección. El contexto debe ser establecido para conocer los criterios dentro de los que los riesgos deben ser administrados.
- Identificación del Riesgo: Es el proceso de encontrar, reconocer y describir los riesgos. Como la identificación de fuentes de riesgos, eventos, causas y consecuencias. Puede incluir datos históricos, opiniones de expertos y necesidades de las partes interesadas.
- Análisis, Evaluación y Valoración de Riesgos: En esta fase se identifican los activos que se quieren proteger y sus debilidades; activos que incluyen procesos, información y datos, también las amenazas a las que están expuestos. Luego de establecer los activos se puede validar si el alcance definido en los posibles controles de tratamiento de riesgos fue el correcto o debe ser ajustado. Adicionalmente, en esta etapa se deben distinguir los tipos de amenazas a presentarse como físicas, lógicas o estratégicas y sus orígenes que podrían ser técnico, humano, accidental o intencional, los daños que pueden implicar las

amenazas, el impacto y la determinación sobre las pérdidas causadas por los riesgos. Los controles serán preventivos, detectivos y correctivos.

- Tratamiento del Riesgo: Es el proceso para modificar el riesgo. Puede incluir evitar, eliminar la fuente del riesgo, compartir, reducir y retener el riesgo. En esta fase se establecen las posibles acciones sobre los riesgos y se define un plan de tratamiento según una priorización. El plan debe definir recursos, responsabilidades y actividades de acuerdo a los recursos económicos, legales, técnicos, operativos, etc. Los controles recomendados deben incluir análisis costo – beneficio tanto de la implementación como del mantenimiento. El plan de tratamiento de riesgos debe incluir la línea de mando requerida para cumplir con las definiciones, los tiempos de vida útil de los activos y dar espacio a la etapa de mejora continua.
- Monitoreo del Riesgo: Implica realizar un seguimiento, control, supervisión, observación crítica y determinación del estado a fin de establecer el cambio del nivel de rendimiento requerido o esperado y lograr que la gestión esté continuamente actualizada para lograr evaluar indicadores de cumplimiento. Con el monitoreo y la mejora continua se asegura la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos definidos. También permite agregar al análisis riesgos nuevos que puedan aparecer.

Priorización e Impacto de los Riesgos

Debido a que el nivel de riesgo es el grado de exposición y el resultado de relacionar la probabilidad con el impacto y los controles que se estén realizando (Álvarez Romero, 2016), no todos los riesgos tienen la misma importancia en términos de su impacto, es por ello que según Baca Urbina (2016) se clasifican en las siguientes prioridades:

- Riesgos de Prioridad 1:

Son los riesgos que en caso de ocurrir terminarían con la ejecución de un proceso, por ejemplo, una mala determinación de la inversión requerida para un proyecto o para la compra de tecnología. Un ejemplo podría ser, la falta de comprometimiento de la alta dirección en un proyecto porque podría pasar demasiado tiempo para que se tomen las decisiones planificadas.

- Riesgo de Prioridad 2:

En esta clasificación están los riesgos externos y por lo tanto la organización no los puede controlar directamente. Un ejemplo podría ser que una empresa está planificando expandir sus operaciones aumentando sucursales pero una crisis económica mundial le impediría ganar mercado debido a la contracción del mismo.

- Riesgo de Prioridad 3:

Son riesgos que al ocurrir causarían perturbaciones o retrasos en la programación, evaluación, implementación u operación, pero no podrían anular un proceso, por ejemplo, podría ser la falta de capacitación o la dificultad para conseguir información para la toma de decisiones o no alinear la TI a la planeación estratégica de la organización.

- Riesgo de Prioridad 4:

Son aquellos riesgos que afectan de forma mínima la programación, evaluación, implementación u operación y podrían ser inconvenientes cotidianos como falta temporal de material para trabajar, retraso en el suministro de recursos, etc.

Umbrales de Tolerancia

Según Baca Urbina (2016) se deben concentrar los esfuerzos en los riesgos de prioridad 1 puesto que los riesgos de prioridad 2, 3 y 4 se los considera molestos y

pueden causar retrasos, pero no ponen en riesgo la viabilidad de un proceso. Además, según el mismo autor, prevenirlos, evitarlos o mitigarlos es relativamente fácil y poco costoso (Baca Urbina, 2016). Un umbral de tolerancia es el valor máximo o mínimo que puede adquirir un factor de riesgo antes de invertir para mitigar sus efectos. Una vez que se han identificado, localizado y definido los umbrales de cada uno de los riesgos, se debe establecer estrategias para evitar que sucedan o que en el caso de ocurrir su impacto sea mínimo.

A la priorización del impacto de los riesgos, debe ir ligado el concepto de umbral de tolerancia debido a que los dos criterios deben mantener un equilibrio antes de decidir invertir en darle tratamiento a los riesgos.

Tratamiento de los Riesgos

El autor Jaramillo (2013) propone las siguientes técnicas de tratamiento de riesgos:

- Evasión del riesgo: Evitarlo, eliminarlo, retirarse de él o no participar.

  Incluye no realizar alguna actividad que podría llevar a correr un riesgo o que podría producir un riesgo. Casi siempre puede parecer la respuesta a todos los riesgos, pero también significa perder una ganancia potencial.

  También se considera reemplazar un activo por otro que no se vea afectado por una amenaza.

- Reducción del riesgo: Optimizarlo, mitigarlo.

  Consiste en reducir la severidad de la pérdida o la probabilidad o frecuencia de la pérdida que se produzca. Reconociendo que los riesgos pueden ser positivos o negativos, la optimización de los riesgos significa encontrar un equilibrio entre el riesgo y el efecto negativo de la operación o actividad y entre la reducción del riesgo y el esfuerzo aplicado.

En condiciones ideales tomar las medidas oportunas para reducir la probabilidad para que el nivel de riesgo se sitúe por debajo del umbral. Se lo hace de dos formas; implementando medidas preventivas en caso de desear reducir la probabilidad y en caso de querer reducir el impacto se establecen controles para las amenazas.

- Compartir: Transferirlo, externalizarlo o asegurarlo.

  Se basa en compartir con otra parte la carga de la pérdida o el beneficio de la ganancia de un riesgo y también las medidas para reducir el riesgo.

- Retención: Aceptarlo, asumirlo.

  Implica la aceptación de la pérdida o del beneficio de la ganancia de un riesgo cuando se produzca. Retener un riesgo es una estrategia viable para los pequeños riesgos donde el costo de asegurarse contra el riesgo sería mayor en el tiempo que las pérdidas totales sufridas. Algunas empresas, a pesar del riesgo, no dejan de aprovechar la oportunidad que para el negocio supone una actividad arriesgada. Todos los riesgos que no se evitan o no se transfieren son retenidos automáticamente o por defecto.

El autor Jaramillo (2013) que realizó su investigación utilizando COBIT 5, también señala que las opciones de tratamiento de los riesgos deben ser evaluadas por el alcance de la reducción del riesgo y el alcance de cualquier beneficio creado. Pueden considerarse y ponerse en práctica algunas opciones ya sea individualmente o combinadas. La selección de la opción idónea parte de la base de considerar el costo de implementar cada opción contra los beneficios derivados de la misma.

Metodologías, Normas y Modelos de Gestión de Riesgos

A continuación, se presentan algunas metodologías de análisis de riesgos (entre normas, marcos metodológicos y estándares) de la investigación realizada por el autor

Baca Urbina (2016). Así también, se muestran normas y modelos investigados por Vanegas y Pardo (2014). Finalmente, se muestran modelos de la obra de Estupiñán Gaitán (2006):

- CITICUS ONE: Software comercial de Citicus[7] que implementa el método FIRM[8]. Software basado en web utilizado para medir el nivel de riesgo sobre los activos, procesos y actividades de una organización.
- CRAMM: Risk Assessment and Management Methodology. Creado por la Agencia Central de Informática y Telecomunicaciones (CCTA). Originalmente desarrollado para el uso del gobierno de Reino Unido, actualmente propiedad de Siemens. Es una metodología de gestión de riesgos que contiene tres etapas como el establecimiento de objetivos, evaluación de riesgos e identificación y selección de contramedidas (CEDIA, 2018).
- MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Es una metodología de Análisis y Gestión de Riesgos de los Sistemas de Información alineada con ISO/IEC 27005 y otras metodologías internacionales (Baca Urbina, 2016). El propósito de este método está relacionado con el uso de medios electrónicos, informáticos y tecnológicos, sujetos a ciertos riesgos que se deben minimizar para mitigar la desconfianza en el uso de estos medios (Vanegas & Pardo, 2014).
- Los volúmenes de MAGERIT[9] incluyen la metodología a implementar, los elementos genéricos para facilitar el proceso y una guía con técnicas para la gestión y análisis de riesgos. Esta metodología consta de cuatro fases: la

[7] Citicus, empresa privada formada en 2000 para desarrollar y vender software de gestión de seguridad y riesgo cuyo software insignia es Citicus ONE.
[8] FIRM, Fundamental Information Risk Management, es una metodología basada en investigación estadística para medir y gestionar el riesgo de la información.
[9] Magerit, Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Se basa en analizar el impacto que puede tener para una empresa la violación de la seguridad buscando identificar amenazas y vulnerabilidades para una identificación de medidas preventivas y correctivas.

planificación del proyecto de riesgos, el análisis de riesgos, la gestión de riesgos y la selección de salvaguardas (Alfaro, 2017).

- ISO 27000: Presenta los requerimientos para una adecuada gestión de seguridad de la información, algunos de sus capítulos relevantes son la ISO 27002 que es una guía de buenas prácticas que describe objetivos de control e indicadores para la seguridad de la información; la ISO 27005 que establece las directrices para la gestión en la seguridad de la información basada en un enfoque de gestión de riesgos; la ISO 27007 consiste en una guía de auditoría de un SGSI o Sistema de Gestión de Sistemas Informáticos; la ISO 27031 que consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones (Baca Urbina, 2016, pág. 49).
- BS 7799-3: Es una norma publicada por el British Standard Institute. Proporciona una guía para soportar los requisitos establecidos por el ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión de riesgos en la construcción de un sistema de gestión de la seguridad de la información (SGSI). El objetivo de la norma es dar efectiva seguridad a la información. Además, incluye la identificación y evaluación del riesgo, a través de la implementación de controles para su reducción, monitoreo, revisión, mantenimiento y mejora continua del sistema basado en el control del riesgo (Baca Urbina, 2016).
- COBIT 5: Es un marco de referencia internacional aceptado por recomendar buenas prácticas para el control interno de la información. Posee un marco de dominios como planificar y organizar; adquirir e implementar; entregar y dar soporte; y monitorear y evaluar (Baca Urbina, 2016).
- CRISC: Es una certificación de ISACA orientada a profesionales de TI que contiene cinco dominios de conocimiento como identificación, evaluación y

estimación de riesgos; respuesta ante riesgos; monitoreo de riesgos; diseño e implementación de controles de sistemas de información; y por último monitoreo y mantenimiento de controles de sistemas de información (Valencia, 2015).

- ISO 27005: Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos (Baca Urbina, 2016).
- ISO 31010: Es una norma publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) enfocada en la gestión de riesgos. El marco de gestión del riesgo de esta norma proporciona políticas, procedimientos, parámetros y disposiciones organizativas que integran la gestión de riesgos en todos los niveles de una organización (Baca Urbina, 2016).
- ITIL: Fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos corporativos, lo que ha dado como resultado la creciente necesidad de servicios informáticos de calidad que correspondan a los objetivos del negocio y las expectativas de los clientes. En este marco metodológico se captó que el énfasis pasó de centrarse en el desarrollo de aplicaciones de TI a la gestión de los servicios de TI (Baca Urbina, 2016).
- OCTAVE: Es una técnica de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en Carnegie Mellon University. Es un conjunto de herramientas, técnicas y métodos para la evaluación del riesgo que tiene en cuenta la definición de los activos como hardware, software, información y sistemas (Baca Urbina, 2016).

Los principales beneficios de esta metodología consisten en que identifica riesgos que pueden impedir la consecución de objetivos, enseña a evaluar los riesgos de seguridad de la información, crea una estrategia para reducir los riesgos de seguridad prioritarios y ayuda al cumplimiento de regulaciones (Alfaro, 2017).

- RISK IT: Es un marco de trabajo a nivel mundial enfocado a las TI y publicado por ISACA. Proporciona una visión global sobre los riesgos empresariales asociados con las actividades relacionadas con TI. Al igual que COBIT 5, RISK IT se centra en el cumplimiento de los objetivos de la organización y puede personalizarse a cualquier tipo de organización. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y compara sus resultados (Baca Urbina, 2016).
- UNE 71504: Es una norma orientada al análisis y gestión de riesgos para los sistemas de información. Esta norma define la gestión de riesgos con base a las fases de caracterización de activos, caracterización de amenazas, cálculo intrínseco del riesgo, caracterización de salvaguardas, cálculo del riesgo efectivo, evaluación de riesgos, tratamiento de riesgos, administración de la gestión de riesgos (Vanegas & Pardo, 2014, págs. 37-39).
- COSO: Committee of Sponsoring Organization of the Treadway, es un marco integrador que se puede aplicar dentro de cualquier organización indistintamente de sus características. Establece cinco componentes de control interno que agrupan 17 principios en representación de conceptos fundamentales para el establecimiento de un efectivo control interno. Para COSO la evaluación de riesgos se considera un proceso dinámico en el que varias personas interactúan para definir los riesgos tanto internos como externos a los cuales se expone a

entidad y puede afectar la consecución de sus objetivos ya sean de operación, información o de cumplimiento (Alfaro, 2017).

- COSO II: Ha desarrollado una estructura conceptual para la administración del riesgo empresarial denominada ERM para el entendimiento de la formulación y seguimiento de un proceso básico en la administración del riesgo como apoyo al gobierno corporativo. Se centra directamente en el logro de los objetivos de la entidad y ésta provee una base para definir la efectividad de la administración del riesgo empresarial. Las empresas deben crear valor, enfrentar y superar las incertidumbres que representan los riesgos y oportunidades y así enriquecer su capacidad para generar valor (Estupiñán Gaitán, 2006).
- COSO III: La diferencia con su predecesor (COSO II) es que no se limita a la fiabilidad de la información financiera, sino que se brindó cabida a todo tipo de información (Alfaro, 2017).
- COSO IV: La diferencia con la versión anterior (COSO III) es que aborda la evaluación de la gestión de riesgos empresariales y la necesidad de las organizaciones de mejorar su enfoque de gestión de riesgos para satisfacer las demandas de un entorno empresarial en evolución (Alfaro, 2017).
- NIST 800-30: Es la guía para la administración de riesgos de tecnologías de información del Instituto Nacional de Estándares y Tecnología (NIST) aplicable a las instituciones gubernamentales de Estados Unidos. Plantea una estructura metodológica basada en nueve fases (Valencia, 2015).
- MEHARI: Es el Método Armonizado de Gestión de Riesgos, Method for Harmonizad Analysis of Risk. Fue desarrollado en Francia desde 1996 con el fin de asistir a los ejecutivos de las organizaciones en sus esfuerzos para gestionar la seguridad de la información y recursos asociados para reducir riesgos (Valencia, 2015).

De todas estas metodologías, normas y modelos de gestión de riesgos se podría destacar RISK IT por promover la gestión de riesgo tecnológico como parte de la cultura de la organización para asumir mayores riesgos y generar rentabilidad, es decir, ir en búsqueda del riesgo. Para lograr lo antes citado, se basa en la gestión del riesgo y en la comunicación acorde a las necesidades de la organización. RISK IT brinda una guía para el flujo de comunicación de tal forma que el riesgo tecnológico se exprese en términos claros e inequívocos. Además, la herramienta se destaca porque es una práctica global, orientada a un público amplio que está involucrado en gestión y uso de tecnología que necesitan una guía para gestionar el riesgo (Gualim, 2014).

Así mismo, COBIT 5 es una herramienta que basada en cinco principios posibilita a la empresa construir una metodología de gobierno y gestión que optimiza la inversión y el uso de la información y de la tecnología para el beneficio de las partes interesadas (ISACA, 2012). Tanto los fundamentos de RISK IT como de COBIT 5 serán utilizados para el presente trabajo de titulación.

Marco de Trabajo

Al decidirse por una metodología o modelo de gestión de riesgos, esta ha de estar plenamente integrada con los procesos de la empresa requiriendo un compromiso por parte de la alta dirección de la misma así como una planificación estratégica dentro de un marco de trabajo, el mismo que debe ser objeto de seguimiento, control y revisión de forma periódica que permita tomar decisiones oportunas para la mejora continua (Instituto Nacional de Ciberseguridad, 2017).

Es deseable que un marco de trabajo interprete a la empresa en su contexto, establezca una política de gestión de riesgos, identifique autoridades y sus competencias, defina la integración en los procesos de negocio como plan estratégico para que sea relevante, prevea los recursos necesarios, establezca mecanizamos de

comunicación. Finalmente, este marco de trabajo, se desarrollará dentro de un calendario y una estrategia de implementación que permita cumplir objetivos, aplicar políticas, cumplir la legislación y normativa, organizar la formación y comunicación de las personas involucradas (Instituto Nacional de Ciberseguridad, 2017)

CAPÍTULO III

Gestión de Riesgos Basado en COBIT 5 y RISK IT

El presente capítulo realizará una recopilación sobre COBIT 5 y RISK IT debido a que son parte del presente trabajo de titulación. Además de ser marcos de referencia internacionales; mismos que apoyan a las empresas para alcanzar las metas propuestas mediante el gobierno y la gestión de TI.

Definición del Contexto

ISACA define que gestionar riesgos es garantizar que se administren las medidas para aprovechar las oportunidades estratégicas de una organización que posee sistemas de información e infraestructura de TI y, además, que se consiga una reducción del riesgo. Un riesgo es una contingencia o proximidad de un daño (ISACA, 2020). El concepto de riesgo ha tenido diversas interpretaciones, pero existe riesgo en cualquier situación en que no se conozca con exactitud lo que ocurrirá a futuro (RAE, 2019).

Para el desarrollo del presente capítulo se tendrá como base los documentos titulados:

- El Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa de COBIT 5 (A Business Framework for the Governance and Management of Enterprise IT).
- Seguidamente, el Marco de Gestión de Riesgos de TI (RISK IT Framework).
- Finalmente, la Guía Enabling Processes (Procesos Catalizadores o Procesos Habilitantes).

Los documentos mencionados son de autoría de ISACA, que es una institución fundada en 1969 con el fin de proveer conocimiento, certificaciones, instrucción sobre

seguridad de sistemas de información, gobierno empresarial, gestión de TI y riesgo relacionado con TI. Los mencionados documentos se tomarán como base que sustente la propuesta de implementación de un marco metodológico para la gestión de riesgos que es el propósito global del presente trabajo de titulación.

En primer lugar, se debe indicar que COBIT 5 es un marco de trabajo genérico, para empresas de distintos tamaños, con o sin ánimo de lucro, e integral para el gobierno y la gestión de las TI en las empresas; construido sobre cinco principios básicos como son (ISACA, 2012):

1. Satisfacer las necesidades de las partes interesadas.
2. Cubrir la empresa extremo a extremo.
3. Aplicar un marco de referencia único e integrado.
4. Hacer posible un enfoque holístico.
5. Separar el gobierno de la gestión.

Dentro de una estructura empresarial el gobierno asegura que se evalúen las necesidades, condiciones y opciones de las partes interesadas (accionistas, proveedores, clientes, ejecutivos del negocio, responsable de riesgos, etc.) para determinar que se alcanzan unas metas corporativas equilibradas y acordadas; ejerciendo la dirección a través de la priorización y la toma de decisiones; y realizando mediciones al rendimiento y cumplimiento respecto a la dirección (ISACA, 2012). Así también, la gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales (ISACA, 2012).

Las empresas han reconocido que el comité o la junta directiva y los ejecutivos deben aceptar a las TI como cualquier otra parte importante del negocio y deben para esto, trabajar juntos de modo que se incluya a las TI en el enfoque de gobierno y de gestión.

COBIT 5 se encarga de gestionar todas las actividades relacionadas con TI en la organización. Estos procesos tienen que ver con eventos internos o externos. Los eventos internos pueden ser incidentes operacionales, fracasos en los proyectos, cambios de las estrategias de TI y fusiones; y, los eventos externos pueden incluir cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías y nuevas regulaciones. Estos eventos traen relacionado un riesgo implícito, pero a la vez traen una oportunidad para evaluar ese riesgo y plantear soluciones oportunas y eficientes. En efecto, el riesgo y todas sus dimensiones es el tema principal que se aborda en el Marco de Gestión de Riesgos de TI, RISK IT (ISACA, 2012).

Un riesgo de TI es también un riesgo del negocio y se compone de eventos relacionados con las TI que pueden afectar potencialmente a ese negocio. Estos eventos pueden ocurrir con una frecuencia incierta a la vez que su impacto o efecto resulta desconocido; como consecuencia, la empresa podría tener dificultades para alcanzar sus metas y objetivos estratégicos. A esta idea se debe aumentar que los riesgos de TI siempre existen sean o no detectados o reconocidos por la organización (ISACA, 2020).

El marco o modelo RISK IT y la gestión de riesgos que propone es una práctica global y un requisito estratégico de cualquier organización, se diferencia de otros marcos y normas existentes que tratan a la gestión de riesgos en que RISK IT cubre todos los riesgos de TI, tal es así que mediante la adopción de RISK IT se aplican automáticamente los principios de ERM, en la tabla 1 se realiza una comparación. Los espacios coloreados en gris oscuro expresan que el aspecto de riesgo está completamente cubierto por la herramienta, los espacios coloreados en gris claro muestran que está parcialmente cubierto y los espacios en blanco no cubren el aspecto (ISACA, 2020).

Tabla 1.

Comparativa de Marcos de Gestión de Riesgos

Aspecto	RISK IT[10]	COSO ERM[11]	ISO 31000:2009[12]	AS/NZS 4360:2004[13]	PMBOK[14]	ISO/IEC 27005:2008[15]
Se alinea con los objetivos del negocio.						
Balancea costos y beneficios en la gestión de riesgos.						
Provee lineamientos para comunicación abierta.						
Establece responsabilidades para operar dentro de los niveles de tolerancia.						
Está disponible para el público en general.						
Posee una visión integral sobre riesgos de TI.						
Posee prácticas de gestión de riesgos para determinadas áreas (gestión de proyectos, de servicios, de seguridad).						
Proporciona un modelo de procesos detallado con directrices de gestión y modelos de madurez.						

Aspecto cubierto
Aspecto parcialmente cubierto
Aspecto no cubierto

Recuperado de: (ISACA, 2020)

[10] RISK IT, herramienta desarrollada por ISACA para apoyar la gestión de riesgos relacionados con TI.
[11] COSO ERM, estudia los factores y brinda recomendaciones sobre gestión de riesgo empresarial (ERM), control interno y disuasión al fraude.
[12] ISO 31000:2009, se trata de un estándar que a través de una serie de directrices y principios busca que una empresa implemente un sistema de gestión del riesgo con el fin de reducir los obstáculos que impiden la consecución de objetivos.
[13] AS/NZS 4360:2004, es una norma para gestión de riesgos donde se proporciona un marco genérico para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar el riesgo.
[14] PMBOK, un conjunto de procesos y áreas de conocimiento que sugieren buenas prácticas dentro de la gestión de proyectos.
[15] ISO/IEC 27005:2008, una norma compatible con los conceptos generales especificados en ISO / IEC 27001 y diseñada para ayudar a la implementación de la seguridad de la información basada en un enfoque de gestión de riesgos.

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

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

1. Gobernar el riesgo (GR).
    - Establecer y mantener una visión o panorama común del riesgo (RG1).
    - Integrar con el ERM o con la gestión de riesgos empresariales (RG2).
    - Tomar decisiones conscientes sobre los riesgos del negocio (RG3).
2. Evaluación del riesgo (ER).
    - Recoger datos (RE1).
    - Analizar los riesgos (RE2).
    - Mantener el perfil de riesgo (RE3).
3. Respuesta ante el riesgo (RR).
    - Articular riesgos (RR1).
    - Manejar riesgos (RR2).
    - Reaccionar a los eventos o acontecimientos (RR3) (ISACA, 2012).

Propósito

La herramienta RISK IT propone que los riesgos de TI son un componente del universo de riesgos a los que está sometida la organización. Por lo tanto, gestiona los riesgos del negocio asociados al uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI dentro de una organización, ese es su propósito general.

Describe eventos relacionados con TI que podrían afectar a la organización. Esto incluye tanto la frecuencia y la magnitud incierta, la creación de problemas en el incumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades (ISACA, 2020). Por tales razones, la herramienta RISK IT es uno de los insumos que aportan al presente trabajo de investigación.

Destinatarios y Beneficios

Según RISK IT de ISACA, el uso común y generalizado de las TI acarrea beneficios para una organización. Debido a su importancia, los riesgos relacionados con las TI deben ser tratados como los demás riesgos clave, tales como los riesgos del mercado, los riesgos de crédito, los riesgos operativos, etc. Muchos de estos riesgos han sido incorporados a las organizaciones en los procesos de toma de decisión, pero algunos ejecutivos tienden a delegar los riesgos a los especialistas técnicos porque podrían no tener una clara comprensión de los riesgos que se asocian a las TI, su priorización y la respuesta a los mismos. Sin embargo, los riesgos no son puramente una cuestión técnica, el conocimiento sobre la gestión del negocio es lo más importante y los gerentes del negocio han de determinar lo que se debe hacer para apoyar ese conocimiento, por consiguiente, son responsables de la gestión de los riesgos asociados (ISACA, 2020). Los elementos descritos aportan al presente trabajo de titulación. Así también, el marco RISK IT incluye a todos los roles, todos los cargos, los líderes y funciones de apoyo tal como se puede observar en la tabla 2, son los llamados destinatarios. Al mismo tiempo, se pueden observar los beneficios que cada rol obtiene con la adopción del marco o modelo:

Tabla 2.

Roles, Destinatarios y Beneficios

Cargo o Rol	Beneficios o razones para usar el marco de riesgos de TI
Junta y dirección ejecutiva	Facilita la comprensión de sus responsabilidades y funciones con respecto a la gestión de riesgos de TI.
Gestores de riesgos	Asiste con la gestión de riesgos de TI.
Administrador de riesgos operacionales	Marca su vinculación con los riesgos de TI, la identificación de pérdidas operativas y el desarrollo de los principales indicadores de riesgos.
Dirección de TI	Facilita la comprensión para identificar y gestionar los riesgos y cómo comunicarlos cuando se han tomado decisiones de negocio.
Director de Servicios de TI	Facilita la comprensión del punto de sus responsabilidades sobre los riesgos de TI.
Administrador de la continuidad del negocio	Facilita el entendimiento sobre la alineación de la gestión de riesgos y la continuidad del negocio.
Administrador de seguridad de TI	Marca el posicionamiento de los riesgos de seguridad.
Director Financiero	Obtiene una visión de los riesgos relacionados con TI y sus implicaciones financieras.
Oficial de Gobierno Organizacional	Asiste con la supervisión de responsabilidades de gobierno de TI.
Director ejecutivo	Comprensión de la gestión de los riesgos entre todos los riesgos corporativos.
Auditores de TI	Permite el análisis de riesgos en apoyo de los planes de auditoría e informes.
Auditores externos	Orienta sobre las tecnologías relacionadas con los niveles de riesgos.
Aseguradores	Apoya en el establecimiento de cobertura de seguro de TI y la búsqueda de acuerdos sobre niveles de riesgos.

Recuperado de: (ISACA, 2020)

El marco de RISK IT aborda algunos beneficios, de ser implementado, los resultados esperados serían (ISACA, 2020):

- Un marco de referencia sobre la forma de gestionar los riesgos relacionados con las TI.
- Comprensión de cómo capitalizar una inversión realizada en un sistema de control interno con TI.
- Un lenguaje común para ayudar a gestionar la relación entre los ejecutivos encargados de adoptar decisiones.
- Un perfil de riesgos para mejor entendimiento y aprovechamiento de los recursos de la organización.

Principios de los Riesgos de TI

El modelo RISK IT se refiere a los riesgos de TI o los riesgos organizacionales relacionados al uso de las TI. La conexión con el negocio se fundamenta en los principios en los que se apoya el modelo y que le permiten a la empresa obtener un control adecuado sobre los riesgos, tal como se indica en la figura 5:

Figura 5.

Principios de los Riesgos de TI

Tomado de: (ISACA, 2020)

En el primer principio que se muestra en la figura, la eficaz gestión de la organización en cuanto a riesgos de TI siempre se conecta con los objetivos de la organización debido a que el riesgo de TI es tratado como un riesgo del negocio logrando que sea integral.

Además de que el riesgo de negocio relacionado con TI es visto desde la protección contra destrucción de valor y también como posible generador de valor para la organización.

El segundo principio tiene que ver con que el gobierno eficaz, alinea la gestión de riesgos de TI con el ERM debido a que los objetivos del negocio y la cantidad de riesgo que la organización está dispuesta a asumir están claramente definidos. Además, que el proceso de toma de decisiones examina una gama de consecuencias y oportunidades. Finalmente, los temas relativos a riesgos están integrados en cada departamento de la estructura de la organización.

En el tercer principio, el gobierno eficaz con respecto a riesgos de TI equilibra los costos y beneficios porque el riesgo es priorizado y los controles se llevan a cabo en base a un análisis del coste y del beneficio.

Para el cuarto principio, la dirección eficaz de riesgos asociados a TI promueve la comunicación abierta sobre los mismos debido a que la información es oportuna, exacta, transparente y sirve como base para la toma de decisiones.

En cuanto al quinto principio, la gestión eficaz de los riesgos establece responsabilidades personales para el funcionamiento dentro de niveles de tolerancia aceptables, esto incluye la rendición de cuentas además de que la cultura de riesgos se promueve de manera activa comenzando por las capas más altas y las decisiones se toman por personas autorizadas.

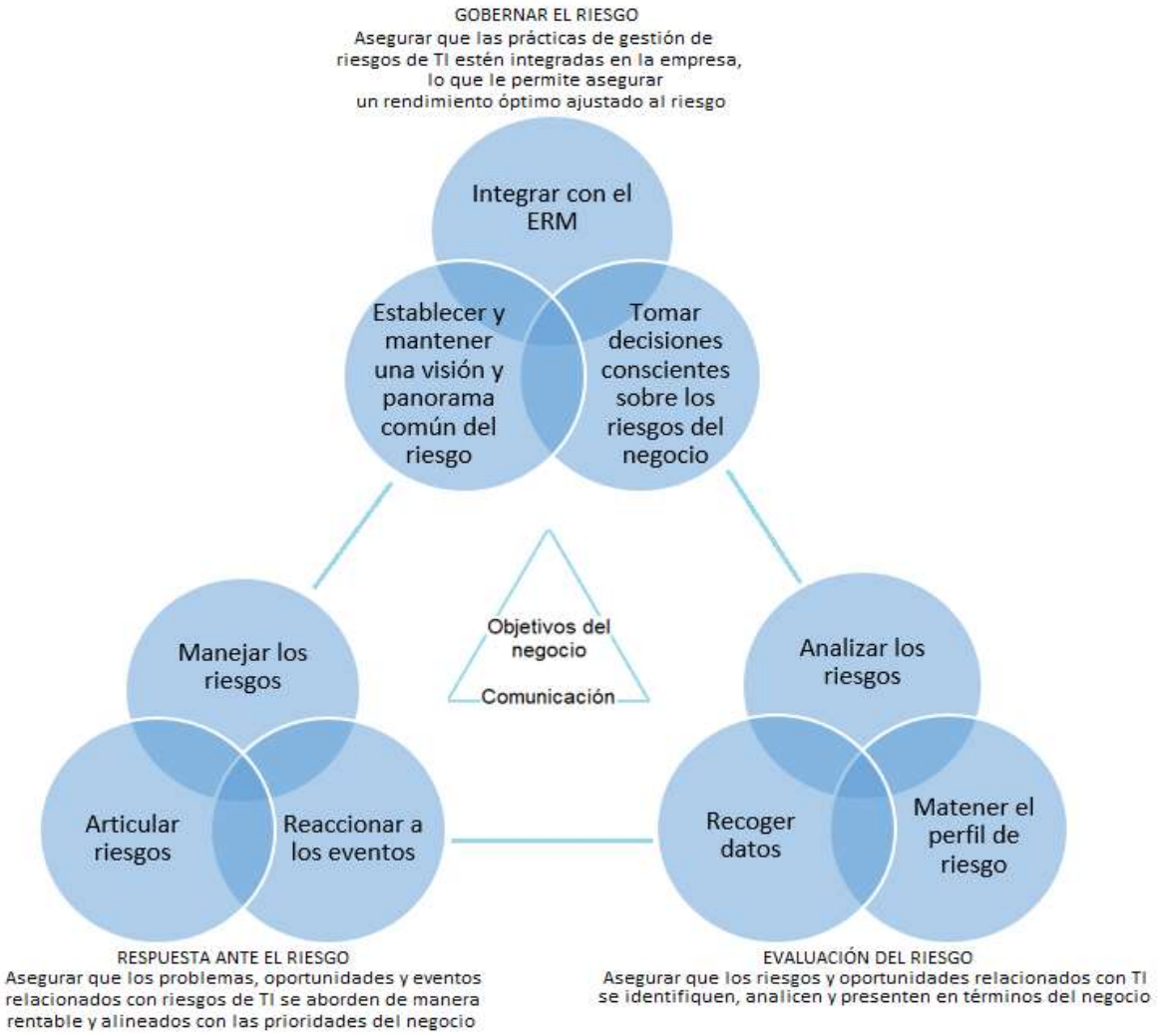
En el sexto y último principio se promueve la gestión de riesgos como una práctica continua por la naturaleza dinámica de los riesgos que son iterativos y significan un permanente proceso en curso al haber cambios que conllevan riesgos. Las prácticas de gestión de riesgos están integradas en orden y prioridad y además son fáciles de aplicar detectando amenazas y tratamiento de las mismas (ISACA, 2020).

Estructura del Marco o Modelo de Riesgos de TI

Una vez descritos los principios instaurados por RISK IT se establece una estructura del modelo de proceso integral de gestión de riesgos, como se indica en la figura 6:

Figura 6.

Estructura del Marco o Modelo de Riesgos de TI



Adaptado de: (ISACA, 2020)

En la figura 6 se muestran los ámbitos de RISK IT que son: Gobernar el riesgo, Evaluación del riesgo y Respuesta ante el riesgo y además se muestran los procesos que son: Establecer y mantener una visión o panorama común del riesgo, Integrar con el ERM o con la gestión de riesgos empresariales, Tomar decisiones conscientes sobre los riesgos del negocio, Recoger datos, Analizar los riesgos, Mantener el perfil de riesgo, Articular riesgos y Manejar riesgos. Tanto los ámbitos como los procesos son la base de la estructura del marco o modelo de gestión de riesgos de RISK IT, a continuación, se explicará cada uno de ellos.

Fundamentos sobre Gobernar el Riesgo

El objetivo de este ámbito es asegurar que las prácticas de gestión de riesgos de TI estén arraigadas en la empresa, lo cual le permite asegurar un rendimiento o rentabilidad óptimos pero ajustado al riesgo.

Los procesos del ámbito gobernar el riesgo son:

- Establecer y mantener una visión o panorama común del riesgo (RG1).
- Integrar con el ERM o con la gestión de riesgos empresariales (RG2).
- Tomar decisiones conscientes sobre los riesgos del negocio (RG3) (ISACA, 2020).

Los componentes esenciales de este ámbito son el apetito y la tolerancia al riesgo, las responsabilidades y rendición de cuentas sobre la gestión de TI, la sensibilización y comunicación y finalmente la cultura de riesgos.

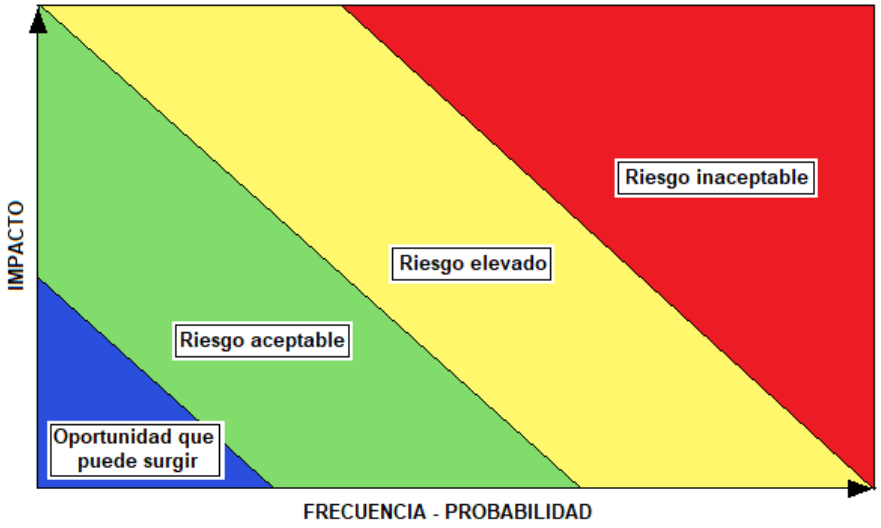
El apetito y la tolerancia por el riesgo son diferentes, el apetito por el riesgo tiene que ver con la cantidad de riesgo que la organización está dispuesta a aceptar mientras que la tolerancia al riesgo es la variación aceptable en relación a conseguir los objetivos.

En cuanto al apetito por el riesgo se deben sopesar dos factores que son: la capacidad objetiva para absorber las pérdidas y la predisposición a asumir riesgos prudentes o agresivos (ISACA, 2020).

El apetito por el riesgo será diferente en cada organización, pero en la práctica se puede definir con la combinación de la frecuencia e impacto del riesgo y suele ser expresado en mapas de riesgos como se puede observar en la figura 7:

Figura 7.

Bandas para Mapas de Riesgos



Adaptado de: (ISACA, 2020)

En la figura 7 se distinguen bandas de colores, el Rojo indica que un riesgo va más allá de su apetito por el riesgo definido como normal. El color Amarillo indica que el riesgo es elevado pero la organización podría aceptarlo, aunque requiere una respuesta adecuada. El color Verde indica un nivel normal aceptable de riesgo y para el que no se necesita acción. Por último, el color Azul que es donde las oportunidades para asumir más riesgos pueden surgir (ISACA, 2020). Este esquema debería enmarcarse en la línea de la cultura de riesgos de la organización.

La tolerancia al riesgo, por su parte, es la desviación desde el nivel establecido por la definición del apetito de riesgo en las políticas de la institución que, por ejemplo, expresa que las actividades deben realizarse dentro de presupuestos y tiempos y se les da un rango para que se puedan considerar dentro de lo tolerable. De este razonamiento se deduce que las organizaciones en las que las políticas son severas podrían carecer de agilidad e innovación para aprovechar las oportunidades del negocio. Por el contrario, existen situaciones en las que las políticas se basan en requisitos legales o reglamentarios en los que es conveniente no ser tolerante al incumplimiento.

La herramienta RISK IT señala que las responsabilidades y rendición de cuentas están relacionadas con las funciones para la gestión de riesgos las mismas que demandan compromiso y por tanto informe de lo actuado, en la tabla 3 se sugieren funciones según el cargo de gobierno, pero dependerá de cada organización aplicarlas de acuerdo a su conformación.

Los espacios marcados de color gris oscuro indican que el rol o cargo lleva responsabilidad principal en un proceso y los espacios coloreadas en gris claro indican que existe una responsabilidad parcial sobre un proceso (ISACA, 2020):

Tabla 3.

Responsabilidades y Rendición de Cuentas sobre los Riesgos de TI

Definición de la función		Gobernar el riesgo			Evaluación del riesgo			Respuesta ante el riesgo		
Función	Definición sugerida	Visión del riesgo	Integrar con el ERM	Decisiones conscientes sobre riesgos	Recoger datos	Analizar riesgos	Mantener el perfil de riesgo	Articular riesgos	Manejar riesgos	Reaccionar a eventos
Consejo	El grupo de altos ejecutivos de la organización responsable de la gestión y control sobre los recursos.									
Director ejecutivo	Funcionario que se encarga de la administración total de la organización.									
Responsable de riesgos	Responsable de supervisar aspectos de gestión de riesgos de la organización.									
Responsable de TI	Responsable de TI para el alineamiento de TI a las estrategias de la organización, la asignación de									

Definición de la función		Gobernar el riesgo			Evaluación del riesgo			Respuesta ante el riesgo		
Función	Definición sugerida	Visión del riesgo	Integrar con el ERM	Decisiones conscientes sobre riesgos	Recoger datos	Analizar riesgos	Mantener el perfil de riesgo	Articular riesgos	Manejar riesgos	Reaccionar a eventos
	recursos y prestación de servicios de TI.									
Responsable financiero	Responsable de la planificación financiera, el mantenimiento de relaciones con los inversores y el control del riesgo financiero.									
Comité de organización de riesgos	Grupo de ejecutivos de la organización comprometido con la colaboración y consenso para apoyar las actividades de gestión de riesgos.									
Propietario de procesos de negocio	Responsable de la identificación de requisitos, diseño y aprobación de gestión de procesos.									

Definición de la función		Gobernar el riesgo			Evaluación del riesgo			Respuesta ante el riesgo		
Función	Definición sugerida	Visión del riesgo	Integrar con el ERM	Decisiones conscientes sobre riesgos	Recoger datos	Analizar riesgos	Mantener el perfil de riesgo	Articular riesgos	Manejar riesgos	Reaccionar a eventos
Responsable de control de riesgos	Responsable de la gestión de dominios específicos de riesgos (jefe de seguridad de la información, continuidad del negocio, recuperación de desastres, cadena de suministro).									
Responsable de recurso humano	Responsable de la planificación y políticas con respecto a los recursos humanos.									
Responsable de cumplimiento y auditoría	Responsable del cumplimiento de funciones y auditoría.									

El cargo conlleva la responsabilidad principal
El cargo lleva la responsabilidad y/o rendición de cuentas parcial
Función no cubierta

Recuperado de: (ISACA, 2020)

La sensibilización y comunicación está relacionada con la concienciación de los riesgos como parte integral de la organización, es decir; denotar que los riesgos de TI se conocen y se entienden dentro de la empresa. Brindan beneficios a la gestión ejecutiva como transparencia para las partes interesadas, pero su ausencia genera una falsa sensación de confianza o la percepción de que la organización podría tratar de encubrir los riesgos (ISACA, 2020).

Fundamentos sobre Evaluación de Riesgo

El objetivo de este ámbito es asegurar que los riesgos y oportunidades relacionadas con TI se identifican, analizan y presentan en términos del negocio.

Los procesos del ámbito evaluación del riesgo son:

- Recoger datos (RE1).
- Analizar los riesgos (RE2).
- Mantener el perfil de riesgo (RE3) (ISACA, 2020).

En este ámbito los componentes son la descripción del impacto de la organización y los escenarios de riesgos de TI.

RISK IT indica que la descripción del impacto de la organización señala que todas las partes interesadas deben tener la capacidad de comprender cómo los eventos adversos o fallos relacionados con TI pueden afectar a los objetivos del negocio, los servicios y los procesos clave del mismo. El vínculo entre la TI y el impacto de escenarios de riesgo organizacional debe ser establecido para comprender los efectos adversos. Es decir, debe existir una traducción del riesgo tecnológico expresado en términos del negocio. Existen varias técnicas basadas en criterios que pueden apoyar a la organización para este propósito:

- COBIT Information Criteria: Expresa cómo los criterios de información de COBIT (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, conformidad y cumplimiento) deben ajustarse para que sean beneficiosos para la organización.
- Balanced Scorecard (BSC): Esta técnica se basa en los objetivos del negocio introducidos por COBIT, pero se estructuran a través de la puntuación del BSC dentro de las perspectivas para evaluar el desempeño de la organización como son clientes; indicadores financieros; procesos internos; y, aprendizaje y crecimiento.
- Extended BSC: Es una variante de la técnica anteriormente descrita, donde se vinculan las perspectivas del BSC a un conjunto limitado de criterios para expresar el riesgo en términos de negocio.
- Westerman: Define al riesgo como el potencial que tiene un acontecimiento imprevisto para amenazar cualquiera de los cuatro propósitos de la organización como son la disponibilidad que mantiene a los sistemas en funcionamiento; la agilidad que es la capacidad para responder con facilidad y velocidad; la precisión que provee información puntual y completa; y, el acceso que garantiza el camino adecuado a los datos y sistemas.
- COSO ERM: Maneja el criterio de estrategia donde los objetivos se alinean a la misión de la organización; de las operaciones que se reflejan en la eficiencia, eficacia, rentabilidad y protección ante la pérdida de recursos; de los informes fiables de información; y del cumplimiento de leyes y reglamentos.
- FAIR: Es el Factor de Análisis de Riesgos de la Información. Divide sus actividades en cuatro etapas como identificar los componentes del escenario de riesgos; evaluar la frecuencia de los eventos que pueden generar pérdidas; evaluar la probable magnitud de las pérdidas; y, por último, derivar y articular el riesgo. Le permite a una organización aplicar, a cualquier activo, la evaluación de

riesgos, observar los riesgos totales de la organización y entender cuánto tiempo y costo involucrará el asegurar la información (Doria, 2014).

Así también que, identificar los escenarios de riesgos es uno de los desafíos para la gestión de riesgos donde se deben observar los riesgos relevantes entre todos los posibles que se relacionan con TI. Además, en la definición de los escenarios se debe lograr cierto realismo, compromiso organizacional, un análisis adecuado y construir la estructura completa de la situación de riesgos. Los escenarios pueden visualizarse desde dos enfoques: un enfoque de arriba hacia abajo en el que se parte de los objetivos del negocio y se realiza un análisis de los escenarios de riesgo relevantes que impacten a esos objetivos y un enfoque de abajo hacia arriba en el que se utiliza una lista genérica de escenarios para definir escenarios más concretos aplicados a la situación particular de la empresa (ISACA, 2020). Pero independientemente del enfoque lo relevante son las categorías de los mismos, RISK IT los clasifica como se indica en la figura 8:

Figura 8.

Categorías de los Factores de Riesgos

Tomado de: (ISACA, 2020)

Para que un escenario de riesgos sea completo debe contener los siguientes componentes: el actor que genera la amenaza, el tipo de amenaza, la acción o evento sobre ese activo dentro del escenario de riesgo, el activo o recurso sobre el cual el escenario actúa, y el tiempo o la duración del evento negativo. Los citados componentes de riesgo se exponen en la figura 9 (ISACA, 2020):

Figura 9.

Componentes de Escenarios de Riesgos

Tomado de: (ISACA, 2020)

El actor es quien genera la amenaza y puede ser externo a la organización o pertenecer a la empresa; el tipo de amenaza puede ser maliciosa, accidental, un fracaso en un proceso o natural; la acción corresponde a un evento concreto como divulgación de información confidencial, interrupción de un proyecto o sistema, el robo, el diseño ineficaz de un proceso, etc.; los activos son los recursos y el tiempo o duración del evento que afecta al activo es relevante para la construcción de escenarios completos para RISK IT.

Fundamentos sobre la Respuesta al Riesgo

El objetivo de este ámbito es asegurar que los problemas, oportunidades y eventos relacionados con los riesgos de TI se aborden de manera rentable y alineados con las prioridades del negocio.

Los procesos del ámbito respuesta frente al riesgo son:

- Articular riesgos (RR1).
- Manejar riesgos (RR2).
- Reaccionar a los eventos o acontecimientos (RR3) (ISACA, 2020).

Según RISK IT, los componentes esenciales del ámbito de la respuesta frente al riesgo son los indicadores de riesgo y la definición con la priorización de la respuesta al riesgo.

Los principales indicadores son capaces de demostrar que la empresa tiene una alta probabilidad de estar sometida a un riesgo que excede el apetito al mismo definido por la organización.

Una empresa puede desarrollar un amplio listado de métricas para servir como indicadores de riesgo, pero los criterios para seleccionarlos incluyen el impacto de los mismos; la facilidad de los indicadores para ser medidos y reportados; la fiabilidad del indicador como vaticinador de riesgo y la sensibilidad del indicador como distintivo para convertirse en riesgo.

El propósito de la definición y priorización de la respuesta al riesgo tiene que ser tal que el futuro riesgo residual (la respuesta al riesgo definida y la respuesta en la práctica) sea tanto como sea posible dentro de los límites de tolerancia frente al riesgo.

Tal como se documentó en el capítulo anterior, RISK IT se acopla con los conceptos generalizados comúnmente para responder y tratar a los riesgos. Lo expresa de la siguiente manera:

- Evitar Riesgos: Significa salir de las actividades o de las condiciones que dan lugar al riesgo. Se aplica cuando no existe una respuesta rentable que pueda tener éxito en reducir la frecuencia y magnitud de un riesgo; o el riesgo no puede ser transferido o compartido; o el riesgo se juzga inaceptable.

- Reducir y Mitigar Riesgos: Se traduce en las medidas que están tomadas para detectar el riesgo seguido por la acción para reducir la frecuencia y el impacto. Las medidas comunes de este tipo de tratamiento son fortalecimiento de la gestión de las prácticas de riesgo de TI e introducción de medidas de control interno para reducir la frecuencia y el impacto de un evento de consecuencias adversas.
- Compartir y Transferir Riesgos: Abarca reducir la frecuencia de riesgos o impacto mediante la transferencia o distribución de una parte del riesgo. Las figuras comunes son la contratación de seguros y la subcontratación.
- Aceptar Riesgos: Significa que la pérdida sea aceptada, esto es diferente a ignorar el riesgo porque aceptar supone que el riesgo es conocido, es decir, una decisión informada se ha aceptado por la dirección o gobierno de la empresa. Si un riesgo particular es evaluado por ser extraordinario y las medidas para reducirlo son prohibitivas se puede decidir aceptarlo (ISACA, 2020).

En adición, la organización tiene que priorizar las respuestas al riesgo utilizando criterios de coste de la respuesta; capacidad para aplicar la respuesta; efectividad de la respuesta para reducir el impacto y la frecuencia del evento adverso; y, eficiencia de la respuesta en relación a los beneficios esperados comparándola con otras inversiones y otras posibles respuestas (ISACA, 2020).

Mejores Prácticas para Gestión de Riesgos

En la tabla 4 se muestra, en general, las mejores prácticas de gestión de riesgos a manera de procesos y actividades que propone RISK IT (Carrillo, 2012).

Tabla 4.

Proceso de Mejores Prácticas de Gestión de Riesgos

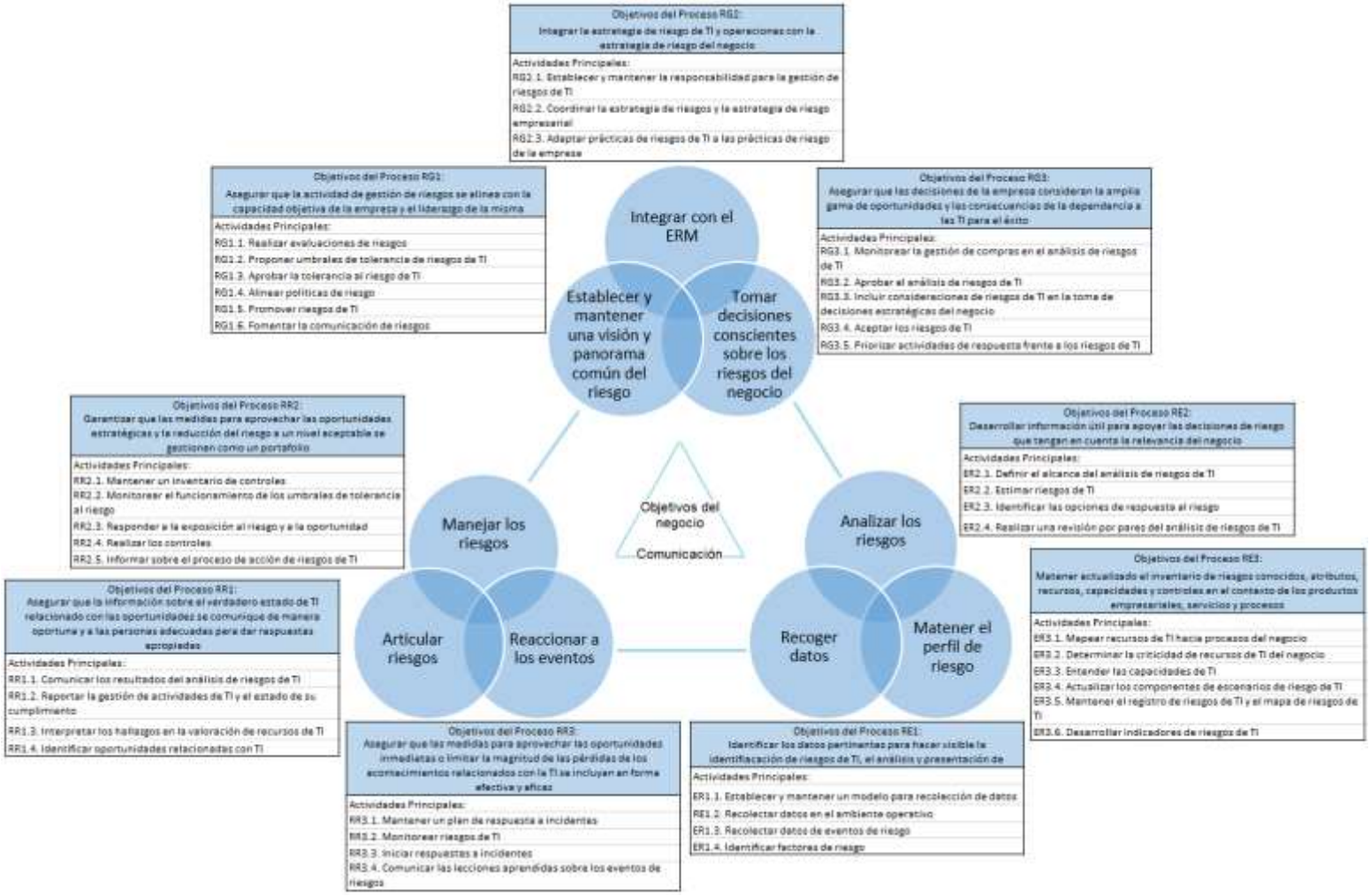
Proceso	Actividades
Generar conciencia del riesgo, comunicación y presentación de informes	Conciencia del riesgo y comunicación del riesgo
	Definir los indicadores del riesgo y presentar informes
	Definir el perfil del riesgo
	Generar una cultura de riesgos
Expresar y describir el riesgo	Expresar el impacto en términos de negocios
	Describir el riesgo, expresar la frecuencia
	Describir el riesgo, expresar el impacto
	Realizar un mapa de riesgos
	Registrar los riesgos
Presentar escenarios de riesgos	Explicar los escenarios de riesgo
	Ejemplificar los escenarios de riesgo

Recuperado de: (Carrillo, 2012)

Visión del Proceso del Modelo o Marco de Riesgos

Figura 10.

Proceso del Modelo o Marco de Riesgos



Adaptado de: (ISACA, 2020)

En la figura 10 se muestra de forma integral los ámbitos de RISK IT, sus procesos, los objetivos y actividades principales dentro del marco o modelo a manera de metodología que utiliza esta herramienta para gestionar riesgos. Existe una visión de los nueve procesos del negocio pertenecientes a los tres ámbitos: gobierno del riesgo, evaluación del riesgo y respuesta al riesgo.

De forma teórica, el modelo comprende los componentes del proceso, las prácticas de gestión y las directrices de gestión (ISACA, 2020):

- Componentes del Proceso: Un proceso efectivo es un conjunto de actividades y controles para realizar una determinada tarea. Los procesos de entrada deben utilizar recursos de acuerdo a las políticas de la empresa y generar una salida.
- Prácticas de Gestión: Las prácticas de gestión son las características necesarias para que los procesos tengan éxito. En escenarios de riesgo, las prácticas de gestión apoyan a las actividades principales. Las prácticas de gestión de riesgos ofrecen un modelo que se puede utilizar para evaluar sus prácticas actuales, determinar dónde existen áreas de mejora y son una guía para las mejoras.
- Directrices de Gestión: Ofrecen sugerencias que las empresas pueden utilizar para implementar procesos de gestión de riesgos de TI y las prácticas en su entorno. Las directrices pueden ayudar con respuestas a preguntas habituales sobre gestión tales como (ISACA, 2020):
    - ¿Cuáles son las principales actividades que deben llevarse a cabo o actividades a mejorar?
    - ¿Qué funciones y responsabilidades deben definirse para que un proceso de gestión de riesgos de TI tenga éxito?
    - ¿Cómo se miden los procesos de gestión de riesgos de TI en una empresa?
    - ¿Cuáles son los indicadores de buen desempeño?

Del mismo modo, se debe recordar que para cada proceso de riesgos de TI se deben considerar:

- Entradas y salidas (como se describió anteriormente en los componentes de un proceso).
- Funciones y responsabilidades: Se especifican en matrices RACI que indican los roles para cada actividad clave, son cargos de la empresa que forman parte del grupo de apoyo para las prácticas de gestión de riesgos de TI, por tal razón se clasifican en: Responsible o comprometido que es el rol que garantiza que las actividades se lleven a cabo con éxito (R); Accountable responsible o el responsable de rendir cuentas porque tiene el recurso necesario y la autoridad para aceptar el resultado de una actividad (A); Consulted o consultado que es el rol que solicita y recibe opiniones sobre una actividad (C); y finalmente, Informed o informado que es quien mantiene actualizado continuamente el progreso de una actividad (I).

A continuación, en la tabla 5, se muestra un ejemplo de matriz RACI, donde se representan las actividades principales de la gestión de riesgos para el caso de análisis de riesgos y los responsables de cada actividad:

Tabla 5.

Ejemplo de Matriz RACI para el Análisis de Riesgos con Actividades Principales

Actividades Principales	CEO	CRO	CIO	CFO	Comité de organización de riesgo	Propietario de procesos de negocio	Responsable de control de riesgos	Responsable recurso humano	Responsable cumplimiento y auditoría
Definir el alcance de riesgos de TI	I	R	C	I	C	R	C		C
Estimar riesgos de TI	I	R	C	C	I	R	R		C
Identificar opciones de respuesta al riesgo		C	C	C	R	R	R		I
Revisar el análisis de riesgos		A-R					I		I

R	Responsable
A	Autoriza
C	Comunica
I	Informa

Recuperado de: (ISACA, 2020)

Como se puede observar en la tabla 5, el definir el alcance de los riesgos de TI (la primera actividad), es responsabilidad del Chief Revenue Officer y Business Process Owner; el cargo que rinde cuentas sobre la actividad es Business Management; los encargados de solicitar y brindar opiniones sobre la actividad son Chief Information Officer, Enterprise Risk Committed, Risk Control Functions y Compliance and Audit; y por último, los cargos que se mantienen actualizados periódicamente sobre la actividad son Chief executive officer y Chief Financial Officer.

Objetivos y métricas: Las métricas pueden ser indicadores que proporcionan una medida de lo que se ha logrado o indicadores que proporcionan una medida de lo que se puede lograr. Las métricas por sí solas no son una solución, pero sí un punto de partida ligado a la madurez debido a que, tomados en conjunto, los objetivos y los indicadores pueden proporcionar elementos para puntuar a la empresa. A continuación, en la tabla 6, se muestra un ejemplo de objetivos y sus respectivas métricas (ISACA, 2020):

Tabla 6.

Ejemplo de Objetivos y Métricas

Objetivos de la Actividad	**Objetivo del Proceso**	**Objetivo del Dominio**
Definir el ámbito del análisis de riesgos de TI	Desarrollar información útil para apoyar las decisiones que sean pertinentes a factores de riesgo del negocio	Asegurar que los riesgos relacionados con TI que se identifiquen se presenten en términos del negocio
Estimar los riesgos de TI		
Identificar las operaciones de respuesta al riesgo		
Métricas de la Actividad	**Métricas del Proceso**	**Métrica del Dominio**
Índice de satisfacción sobre el análisis de riesgos derivados de la	Porcentaje de riesgos sometidos a revisión por pares antes de ser enviados a la dirección	Grado de impacto de los incidentes relacionados con eventos no identificados por

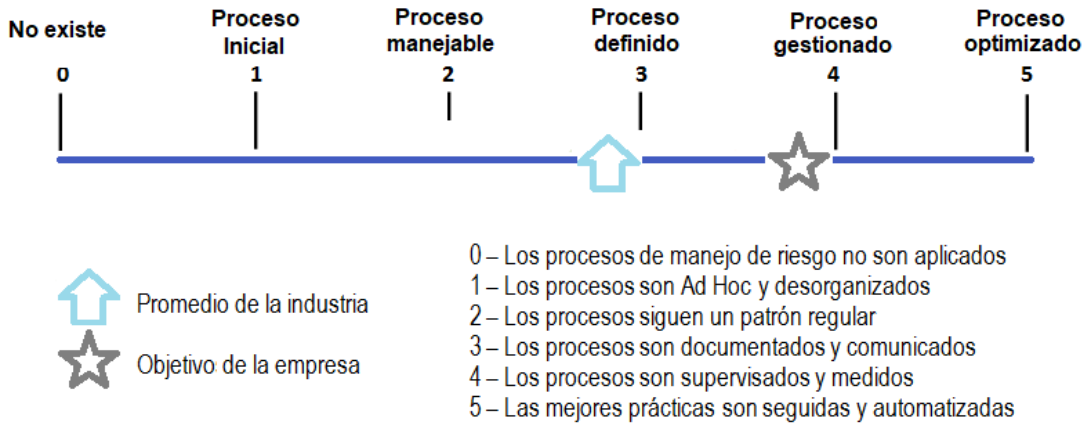
presentación de informes		los procesos de evaluación de riesgos
Porcentaje de evaluaciones realizadas por diferentes analistas que consiguen los mismos resultados	Proporción de pérdidas reales versus pérdidas esperadas	
Porcentaje de evaluaciones realizadas por analistas entrenados		

Recuperado de: (ISACA, 2020)

Del mismo modo, RISK IT propone modelos o niveles de madurez donde se pueden identificar las descripciones de su actual estado o posibles futuros estados. Cada empresa debe reconocer que sus procesos se encuentran en distintos niveles de madurez para poder identificar el rendimiento actual de la organización y en qué nivel la organización desea estar. Las escalas de los niveles de madurez se presentan de la siguiente manera (ISACA, 2020):

Figura 11.

Escalas de los Niveles de Madurez



Tomado de: (ISACA, 2020)

La escala de la figura 11 es incremental de cero a cinco, a continuación, se explican a detalle los niveles:

- Nivel 0 o No Existe, en este nivel la empresa aún no ha adoptado las prácticas básicas de gestión de riesgos de TI. La organización no ha reconocido los riesgos y por consiguiente no existe comunicación alguna sobre los mismos. Entonces no se tiene conciencia de la implementación de controles y tampoco se cuenta con la capacidad para reaccionar ante los riesgos.
- Nivel 1 o Proceso Inicial, en este nivel los procesos son ad hoc, la empresa reconoce la necesidad de reaccionar ante los riesgos, sin embargo, se limita a evitarlos o transferirlos compartiéndolos con algún proveedor o adquiriendo algún seguro, no se considera eliminar los riesgos. Algún éxito en tema de riesgos se debe a la competencia de los responsables y no al apego a procesos definidos y aprobados por tanto se expone a la empresa a aceptar riesgos fuera de los umbrales de tolerancia aceptables.
- Nivel 2 o Proceso Manejable, en este nivel existe una suerte de ordenamiento, se tiene conciencia de las amenazas para reaccionar ante el riesgo si es que se fuera a materializar, existe una comunicación de los riesgos. La empresa cuenta con procesos definidos involucrándose a las partes interesadas, se monitorea, controla, revisa y evalúa de acuerdo a los criterios definidos en los procedimientos. Existe un líder emergente para dar respuesta al riesgo. En este nivel es posible que se detecten deficiencias en los controles que no son atendidos de forma oportuna.
- Nivel 3 o Proceso Definido: En este nivel, debido a que se tiene una conciencia de las amenazas, se comprende el impacto que representan para el negocio. Los procesos se encuentran documentados y son comunicados a los distintos niveles de la organización. El nivel tres requiere una clara definición de procesos

planteando su propósito, sus entradas, actividades, roles, pasos para la verificación y salidas. Se corrigen las deficiencias en los controles de forma oportuna, las correcciones están expresadas en las políticas de la empresa. Se capacita al personal constantemente en materia de gestión de riesgos y en relación a las actividades coherentes con sus respectivos cargos.

- Nivel 4 o Proceso Gestionado Cuantitativamente, en este nivel la organización cuenta con un proceso de gestión de riesgos planificado, supervisado y ajustado. Existe el involucramiento de la alta gerencia y con el asesoramiento de los cargos que realizan gestión de TI determinan si una situación de riesgo se encuentra en el umbral de tolerancia. Por ser gestionado cuantitativamente se cuenta con un proceso de medición de la eficiencia y eficacia de respuesta al riesgo que se encuentra articulado a los objetivos estratégicos del negocio. En este nivel existe una mejora y redefinición que permite actualizar la gestión de riesgos de forma continua, para esto se aplican controles para alcanzar mejores resultados.
- Nivel 5 u Optimizado, la empresa es capaz de cuantificar el valor de la gestión de riesgos, la evaluación y la capacidad de respuesta a los mismos de manera madura y tiene los medios para mejorar de manera continua. Se cuenta con una estrategia para responder al riesgo y se aplican controles con visión de costo y beneficio. El nivel cinco fomenta la mejora de las capacidades de la empresa sobre una clara definición de objetivos individuales y organizacionales. Se implementan tecnologías que permiten asumir nuevas oportunidades para analizar impactos y beneficios de tolerar el riesgo y mantenerlos bajo los umbrales definidos (ISACA, 2020).

En este contexto, en las tablas 7, 8 y 9, se muestran los niveles de madurez que establece RISK IT para los tres ámbitos o dominios gobernar el riesgo, evaluación del riesgo y respuesta ante el riesgo (ISACA, 2020):

Tabla 7.

Niveles de Madurez del Dominio o Ámbito Gobernar el Riesgo (GR)

0 - No existe
La organización no ha reconocido la necesidad de considerar el impacto en el negocio de los riesgos de TI. Las decisiones que implican la aceptación de riesgos de TI cuando tienden a basarse en la falta de información o información incorrecta. No hay conciencia de los de riesgos de TI y la integración con la gestión de riesgos empresariales.
1 – Inicial
Existe conciencia de que el riesgo de TI es importante y debe ser gestionado, pero es visto como un problema técnico. Los criterios de identificación de riesgo de TI varían en toda la organización. El apetito por el riesgo y la tolerancia sólo se consideran en las evaluaciones de riesgos cuando suceden los eventos. Las políticas de empresa y las normas, que son mínimas Las habilidades de gestión de riesgos de TI pueden existir sobre una base apropiada pero no son desarrolladas activamente.
2 – Manejable
Existe conciencia de la necesidad de controlar activamente los riesgos de TI, pero la atención se centra en el cumplimiento técnico sin previsión del valor añadido. Hay líderes emergentes para la gestión de riesgos de TI dentro de los departamentos quienes asumen la responsabilidad y suelen ser considerados responsables, incluso si no hay un acuerdo formal. La tolerancia del riesgo se establece a nivel local. Existe necesidad de orientación de la junta directiva para la gestión de riesgos. Existen inventarios de TI sobre cuestiones de riesgo.
3 – Definido
La gestión de riesgos se ve como una cuestión empresarial y tanto las desventajas como las ventajas de los riesgos de TI son reconocidas. Hay un líder designado para los riesgos de TI en toda la empresa, este líder está comprometido con el Comité de riesgos de la empresa, donde los riesgos de TI están al alcance y son discutidos. La empresa entiende cómo se integra a nivel mundial la perspectiva de riesgo. La tolerancia al riesgo de la empresa se deriva de la tolerancia local y las actividades de gestión de riesgos de TI están siendo alineadas en toda la empresa. La formación sobre sensibilización de riesgos incluye las situaciones y escenarios más allá de políticas específicas y un lenguaje común para la comunicación de riesgos. Existen requisitos definidos para un inventario de los problemas de riesgo. Se cuenta con herramientas para optimizar la reducción de riesgos.
4 – Gestionado
La gestión de riesgos se ve como un facilitador de negocios. El líder designado para los riesgos de TI en toda la organización está plenamente comprometido con el comité de riesgo de la

empresa que espera que sus opiniones aporten valor en la toma de decisiones. El papel del departamento de TI en la gestión del riesgo operacional y la gestión del riesgo empresarial está entendido. El comité de riesgo define el apetito de riesgo y la tolerancia para todos los departamentos, incluidos los riesgos de TI. Las políticas de la empresa y las normas reflejan la tolerancia al riesgo empresarial. Se planifican prudentemente los escenarios de riesgo considerando los riesgos de TI en toda la empresa. Las principales decisiones de riesgo se toman considerando plenamente la probabilidad de pérdida y de recompensa.
5 – Optimizado
Los altos ejecutivos consideran en sus decisiones todos los aspectos de riesgos de TI. El líder del riesgo se considera un asesor de confianza durante el diseño e implementación de operaciones. El departamento de TI es un actor importante en la línea de los esfuerzos empresariales de riesgo operacional. Los objetivos estratégicos se basan en un entendimiento a nivel ejecutivo de TI sobre las amenazas relacionadas con el negocio, los escenarios de riesgo y las oportunidades. La empresa exige formalmente la mejora continua de la gestión de las capacidades de los riesgos de TI basada en objetivos claramente definidos. Existe seguimiento en tiempo real de los eventos y control al igual que la automatización.

Recuperado de: (ISACA, 2020)

Tabla 8.

Niveles de Madurez del Dominio o Ámbito Evaluación del Riesgo (RE)

0 - No existe
La empresa no ha reconocido la necesidad de entender cómo los eventos relacionados con TI y las condiciones (factores de riesgo) pueden afectar su rendimiento. Existe carencia de datos fuerza a asumir aspectos clave del entorno de riesgo durante la toma de decisiones y operaciones en curso.
1 – Inicial
El reconocimiento de la necesidad de la evaluación del riesgo está surgiendo, sin embargo, existe una mínima comprensión del entorno empresarial y los eventos asociados a fin de que las amenazas puedan afectar el desempeño. La información actual sobre los riesgos de TI y las opciones de mitigación se deducen de la evaluación de los eventos ocurridos. Las habilidades de análisis de riesgos de TI pueden existir sobre una base apropiada, pero no están desarrollando activamente.
2 – Manejable
Los escenarios de pérdida son el enfoque de los debates, aunque los principales factores de estos escenarios pueden no ser entendidos. Los individuos asumen la responsabilidad tanto de la evaluación de riesgos y respuesta a los mismos. El análisis de escenarios es apropiado

y se concentra en un número limitado de actividades empresariales. Los enfoques de análisis de riesgo específicos y las herramientas existen, pero se basan en las soluciones desarrolladas por personas clave.

3 – Definido

Hay una comprensión de los fundamentos de riesgo emergentes. Las diferencias entre las TI y los riesgos relacionados con la oportunidad y el apetito de riesgo global están siendo reconocidos. La responsabilidad y rendición de cuentas de las prácticas fundamentales de la evaluación de riesgo se definen. Los procedimientos de análisis de escenarios se establecen y se realizan a través de actividades múltiples, líneas del negocio y productos. Instrumentos de recolección de datos se afianzan a los estándares definidos.

4 – Gestionado

El análisis del riesgo ha sido aceptado como una forma de comprender la resistencia de la empresa y estar preparados para alcanzar los objetivos estratégicos. Todos los tipos de riesgos tienen un responsable designado, la alta dirección empresarial y la gestión de TI en conjunto, determinan la pertinencia de los factores de riesgo del negocio. La evaluación de la eficiencia y eficacia de los riesgos son medidos y comunicados y relacionados con los objetivos de negocio y el plan estratégico de TI. Todos los resultados del análisis están sujetos a revisión por pares y la causa de los problemas de calidad se investiga. La empresa se ocupa del desarrollo a largo plazo de las necesidades de personal con alto potencial en la evaluación de riesgos. Se aplicarán herramientas de análisis de riesgo con un plan estándar.

5 – Optimizado

Los responsables de las decisiones disponen de la mejor información posible acerca de las probabilidades de riesgos, pérdidas y oportunidades. Los factores decisivos de los riesgos reales en las operaciones se comunicarán en toda la empresa. Los empleados en todos los niveles asumen la responsabilidad directa para determinar la pertinencia de los factores de riesgo del negocio. La empresa mantiene un equilibrio óptimo entre los métodos cualitativos y cuantitativos de apoyo en la gestión de la incertidumbre y aprovecha las oportunidades de riesgo. Las actividades de evaluación de riesgos se basan en un conjunto amplio y profundo de los riesgos de TI, escenarios que integran todas las actividades de negocios, líneas de negocio, productos y tipos conocidos de riesgo. La empresa exige formalmente la mejora continua de la recolección de datos, análisis de riesgos y perfiles de competencias. Las herramientas automatizadas permiten el apoyo y la mejora de los esfuerzos para la evaluación de riesgos.

Recuperado de: (ISACA, 2020)

Tabla 9.

Niveles de Madurez del Dominio o Ámbito Respuesta ante el Riesgo (RR)

0 - No existe
La organización no ha reconocido la necesidad de administrar las cuestiones de riesgos. No hay procesos de comunicación de crisis adecuados. El seguimiento de control interno no existe. No hay conciencia de los requisitos externos para implementar los controles, capacidades y recursos para limitar la frecuencia y el impacto (magnitud de la pérdida) de los acontecimientos relacionados con las TI.
1 – Inicial
El reconocimiento de la necesidad de una respuesta frente al riesgo está surgiendo. Existe una responsabilidad mínima para garantizar que las medidas razonables de respuesta frente a los riesgos sean apropiadas. Eventos de TI y condiciones que podrían afectar el día a día de las operaciones en ocasiones se discuten en las reuniones de gestión, pero las respuestas frente a riesgos específicos no se consideran. Los controles de TI existen, pero se basan en requisitos de cumplimiento. La falta de habilidades y competencias para la respuesta al riesgo puede obligar a la empresa a aceptar el riesgo más allá de los niveles de tolerancia.
2 – Manejable
Para la dirección de la empresa existe conciencia de las amenazas cuando se materializan. Existe un líder emergente para la respuesta al riesgo de TI que asume la responsabilidad para mitigar los riesgos y ayudar a gestionar el impacto de los acontecimientos. Deficiencias de control pueden ser identificadas, pero no se remedian en forma oportuna. Los procesos de reducción del riesgo están comenzando a ponerse en práctica cuando se detectan problemas de TI. Existen enfoques comunes para el uso de herramientas de mitigación y respuesta al riesgo, pero se basan en las soluciones desarrolladas por individuos clave.
3 – Definido
A través de la organización hay comprensión individual del impacto de las amenazas y las acciones específicas a tomar en caso de que se materialicen. Se definen responsabilidades y rendición de cuentas para las prácticas de respuesta al riesgo. Las deficiencias de control son identificadas y remediadas de manera oportuna. Los empleados son capacitados periódicamente en amenazas relacionadas con TI, los escenarios de riesgo y los controles pertinentes a sus funciones y responsabilidades. Un plan se ha definido para uso y normalización de las herramientas para automatizar las actividades de reducción del riesgo.
4 – Gestionado
Existe comprensión individual y organizativa de todos los criterios para responder a los riesgos. La alta dirección empresarial y la gestión de TI en conjunto, determinan si una

condición de riesgo es superior a la tolerancia definida de riesgo. La eficiencia y la eficacia de la respuesta a los riesgos son medidas y comunicadas; y, vinculadas a los objetivos del negocio y al plan estratégico de TI. Los criterios son continuamente actualizados para todas las áreas en respuesta al riesgo, incluyendo la articulación de riesgos, mitigación de riesgos, reacción a los acontecimientos y aprovechamiento de oportunidades. Las herramientas se utilizan en las principales áreas para permitir la gestión del riesgo y supervisar los controles críticos, las capacidades y recursos.
5 – Optimizado
Los factores decisivos en los riesgos reales de operaciones se comunican en toda la empresa. La gama completa de estrategias de respuesta al riesgo es aplicada de manera integral, controles costo-eficacia mitigan la exposición al riesgo en forma continua. La empresa exige formalmente la mejora continua de las capacidades de respuesta al riesgo. La empresa emplea tecnologías de respuesta al riesgo para asumirlo y aprovechar las oportunidades competitivas.

Recuperado de: (ISACA, 2020)

En las tablas 7, 8 y 9, lo que se puede deducir como un aporte de la herramienta es que para cada ámbito: gobernar el riesgo, evaluación del riesgo y respuesta ante el riesgo, RISK IT ha establecido una medida específica de diagnóstico actual y además permite una definición de las actividades requeridas para alcanzar el nivel de madurez deseado.

Adicionalmente, se aborda la guía de COBIT 5 titulada Procesos Catalizadores o Procesos Habilitadores. Para analizarla se debe partir de que el modelo de referencia de COBIT 5 contiene un conjunto de 37 procesos de gobierno y gestión clasificados en áreas clave (ISACA, 2019):

- Evaluar, orientar y supervisar.
- Alinear, planificar y organizar.
- Construir, adquirir e implementar.
- Entregar, dar servicio y soporte.
- Supervisar, evaluar y valorar.

Figura 12.

Modelo de Referencia de Procesos de COBIT 5

Tomado de: (ISACA, 2012)

En la figura 12 se distinguen los procesos tanto de gobierno como de gestión de COBIT 5. Los procesos de gobierno están relacionados con evaluar, orientar, supervisar y los procesos de gestión son coherentes con planificar, construir, ejecutar y supervisar.

Se realizó un análisis de la guía de Procesos Catalizadores y se extrajo, para el presente trabajo de titulación todo lo relacionado con riesgos y la gestión de los mismos (son los procesos con recuadro rojo de la figura 12):

- Asegurar la Optimización del Riesgo (EDM03):

Tabla 10.

Proceso Catalizador Asegurar la Optimización del Riesgo

EDM03 Asegurar la Optimización del Riesgo	Área: Gobierno Dominio: Evaluar, Orientar y Supervisar
Descripción del Proceso Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	
Declaración del Propósito del Proceso Asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la tolerancia de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06 Transparencia de los costes, beneficios y riesgos de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
15 Cumplimiento de las políticas internas por parte de las TI	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de partes interesadas que comprenden las políticas • Porcentaje de políticas soportadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de las políticas
Metas y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos.	• Nivel de alineamiento entre riesgo TI y riesgo de negocio • Número de potenciales riesgos TI identificados y gestionados • Frecuencia de refresco de la evaluación de los factores de riesgo
2. La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente.	• Porcentaje de proyectos de la empresa que consideran el riesgo TI • Porcentaje de planes de acción de riesgo TI ejecutados en tiempo • Porcentaje de riesgos críticos que han sido eficazmente mitigados
3. Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado.	• Nivel de impacto empresarial inesperado • Porcentaje de riesgos TI que exceden el riesgo empresarial tolerado

Recuperado de: (ISACA, 2019)

En la tabla 10 se describe el propósito del proceso, una orientación sobre cómo deberá ser ejecutado para la consecución de un conjunto de principales metas de TI. Además, se muestran las metas y métricas del proceso como tal. De la misma forma, en la tabla 11 consta la matriz RACI para el proceso descrito con anterioridad, contiene las respectivas prácticas clave y los roles o cargos apoderados de esas actividades.

Tabla 11.

Tabla RACI para el Proceso Catalizador Asegurar la Optimización del Riesgo

EDM03 RACI Chart																									
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
EDM03.01 Evaluar la gestión de riesgos.	A	R	C	C	R	C	R			I	R	C		I	C	C	C	R	C							C
EDM03.02 Orientar la gestión de riesgos.	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I	I	I
EDM03.03 Supervisar la gestión de riesgos.	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	I	I	C

Recuperado de: (ISACA, 2019)

Igualmente, se muestran las prácticas de gobierno recomendadas para esa práctica clave de gobierno y sus actividades en las tablas 12, 13 y 14:

Tabla 12.

Práctica de Gobierno para Actividad Clave Evaluar la Gestión de Riesgos

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gobierno	**Entradas**		**Salidas**	
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.	**De**	**Descripción**	**Descripción**	**A**
	APO12.01	Factores y problemas de riesgos emergentes	Guías de apetito de riesgo	APO12.03
			Niveles de tolerancia de riesgo aprobados	APO12.03
	Fuera del Ámbito de COBIT	Principios de la gestión de riesgos de la empresa	Evaluación de las actividades de gestión de riesgo	APO12.01
Actividades				
1. Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).				
2. Evaluar y aprobar propuestas de umbrales de tolerancia al riesgo TI frente a los niveles de riesgo y oportunidad aceptables por la empresa.				
3. Determinar el grado de alineación de la estrategia de riesgos de TI con la estrategia de riesgos empresariales.				
4. Evaluar proactivamente los factores de riesgo TI con anterioridad a las decisiones estratégicas de la empresa pendientes y asegurar que las decisiones de la empresa se toman conscientes de los riesgos.				
5. Determinar si el uso de TI está sujeto a una valoración y evaluación de riesgos adecuada, según lo descrito en estándares nacionales e internacionales relevantes.				
6. Evaluar las actividades de gestión de riesgos para garantizar su alineamiento con las capacidades de la empresa para las pérdidas relacionadas con TI y la tolerancia de los líderes a los mismos.				

Recuperado de: (ISACA, 2019)

Tabla 13.

Práctica de Gobierno para Actividad Clave Orientar la Gestión de Riesgos

Práctica de Gobierno	Entradas		Salidas	
EDM03.02 Orientar la gestión de riesgos. Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.	**De**	**Descripción**	**Descripción**	**A**
	AP012.03	Perfil de riesgo agregado incluyendo el estado de las acciones de gestión del riesgo	Políticas de gestión de riesgos	AP012.01
			Objetivos claves a ser monitorizados por la gestión de riesgos	AP012.01
	Fuera del Ámbito de COBIT	Perfiles y planes de mitigación de la Gestión del Riesgo de la Empresa (ERM)	Proceso aprobado para la medición de la gestión de riesgos	AP012.01
Actividades				
1. Promover una cultura consciente de los riesgos TI e impulsar a la empresa a una identificación proactiva de riesgos TI, oportunidades e impactos potenciales en el negocio.				
2. Orientar la integración de las operaciones y la estrategia de riesgos de TI con las decisiones y operaciones empresariales estratégicas.				
3. Orientar la elaboración de planes de comunicación de riesgos (cubriendo todos los niveles de la empresa), así como los planes de acción de riesgo.				
4. Orientar la implantación de mecanismos apropiados para responder rápidamente a los riesgos cambiantes y notificar inmediatamente a los niveles adecuados de gestión, soportados principios de escalado acordados (qué informar, cuándo, dónde y cómo).				
5. Orientar para que el riesgo, las oportunidades, los problemas y preocupaciones puedan ser identificadas y notificadas por cualquier persona en cualquier momento. El riesgo debe ser gestionado de acuerdo con las políticas y procedimientos publicados y escalados a los decisores relevantes.				
6. Identificar los objetivos e indicadores clave de los procesos de gobierno y gestión de riesgos a ser monitorizados y aprobar los enfoques, métodos, técnicas y procesos para capturar y notificar la información de medición.				

Recuperado de: (ISACA, 2019)

Tabla 14.

Práctica de Gobierno para Actividad Clave Supervisar la Gestión de Riesgos

EDM03 Prácticas, Entradas/Salidas y Actividades del Proceso *(cont.)*				
Práctica de Gobierno	**Entradas**		**Salidas**	
EDM03.03 Supervisar la gestión de riesgos. Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	**De**	**Descripción**	**Descripción**	**A**
	AP012.02	Resultados del análisis de riesgos	Acciones correctivas para tratar las desviaciones en la gestión del riesgo	AP012.06
	AP012.04	• Oportunidades para la aceptación de un mayor riesgo • Resultados de las evaluaciones de riesgos de terceras partes • Análisis de riesgos e informes de perfil de riesgos para las partes interesadas	Problemas de la gestión de riesgos para la Dirección	EDM05.01
Actividades				
1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.				
2. Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.				
3. Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.				
4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.				

Recuperado de: (ISACA, 2019)

Luego, la guía sugiere estándares, modelos y marcos relacionados que pueden ser utilizados para controlar el riesgo o para gestionarlo como se muestra en la tabla 15.

Tabla 15.

Guías Relacionadas para el Proceso Catalizador Asegurar la Optimización del Riesgo

EDM03 Guías Relacionadas	
Estándar Relacionado	**Referencia Detallada**
COSO/ERM	
ISO/IEC 3100	Marco de Referencia para la Gestión de Riesgos
ISO/IEC 38500	
King III	• 5.5. TI debería formar una parte integral de la gestión de riesgos de la empresa. • 5.7. El comité de riesgos y el comité de auditoría deberían ayudar a Consejo en el cumplimiento de sus responsabilidades en TI.

Recuperado de: (ISACA, 2019)

- Gestionar el Riesgo (APO12):

Tabla 16.

Proceso Catalizador Gestionar el Riesgo

APO12 Gestionar el Riesgo	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	
Declaración del Propósito del Proceso Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.	
El proceso apoya la consecución de un conjunto de principales metas TI:	
Meta TI	**Métricas Relacionadas**
02 Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de reputación • Número de asuntos de incumplimiento relacionados con TI reportados a la junta que llegan a ser de dominio público o que provocan situaciones de escándalo • Número de asuntos de incumplimiento relacionados con acuerdos contractuales con proveedores de servicio TI • Cobertura de la evaluación del cumplimiento
04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06 Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. • Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.
10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías
13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Número de programas que necesitan ser revisados significativamente debido a defectos de calidad • Coste del mantenimiento de aplicaciones respecto al coste total de TI
Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El riesgo relacionado con TI está identificado, analizado, gestionado y reportado.	• Grado de visibilidad y reconocimiento en el entorno actual • Número de eventos de pérdida con características clave, capturados en repositorios • Porcentaje de auditorías, eventos y tendencias capturados en repositorios
2. Existe un perfil de riesgo actual y completo.	• Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo • Completitud de atributos y valores en el perfil de riesgo
3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	• Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado • Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos
4. Las acciones de gestión de riesgos están efectivamente implementadas.	• Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados • Número de medidas que no reducen el riesgo residual

Recuperado de: (ISACA, 2019)

En la tabla 16 se describe el propósito del proceso, una orientación sobre cómo deberá ser ejecutado para la consecución de un conjunto de principales metas de TI. Además, se muestran las metas y métricas del proceso como tal.

De la misma forma, en la tabla 17 consta la matriz RACI para el proceso descrito con anterioridad, contiene las respectivas prácticas clave y los roles o cargos apoderados de esas actividades.

Tabla 17.

Tabla RACI para el Proceso Catalizador Gestionar el Riesgo

Matriz RACI APO12

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
APO12.01 Recopilar datos.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analizar el riesgo.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Mantener un perfil de riesgo.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Expresar el riesgo.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Definir un portafolio de acciones para la gestión de riesgos.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Responder al riesgo.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Recuperado de: (ISACA, 2019)

Así también, se muestran las prácticas de gobierno recomendadas para esa práctica clave de gobierno y sus actividades en las tablas 18, 19, 20, 21, 22 y 23:

Tabla 18.

Práctica de Gobierno para Actividad Clave Recopilar Datos

APO12 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	EDM03.01	Evaluación de actividades de gestión de riesgos	Datos en el entorno de operación relacionados con el riesgo	Interno
	EDM03.02	• Procesos aprobados para medir la gestión de riesgos • Objetivos clave a ser monitorizados por la gestión de riesgos • Políticas de gestión de riesgos	Datos en eventos de riesgo y en factores contribuyentes	Interno
	APO02.02	Brechas y riesgos relacionados con capacidades actuales	Elementos y factores de riesgo emergentes	EDM03.01 APO01.03 APO02.02
	APO02.05	Evaluación del riesgo		
	APO10.04	Riesgo de entrega de proveedores identificado		
	DSS02.07	Estado de incidentes e informe de tendencias		

APO12.01 Actividades
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con riesgo de TI, dando cabida a múltiples tipos de eventos, múltiples categorías de riesgo de TI y múltiples factores de riesgo.
2. Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.
3. Medir y analizar los datos históricos de riesgo de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria – basados en eventos registrados, bases de datos y acuerdos de la industria sobre divulgación de eventos comunes.
4. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes, problemas e investigaciones.
5. Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples.
6. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.
7. Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.

Recuperado de: (ISACA, 2019)

Tabla 19.

Práctica de Gobierno para Actividad Clave Analizar el Riesgo

Práctica de Gestión	Entradas		Salidas	
APO12.02 Analizar el riesgo. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.	De	Descripción	Descripción	A
	DSS04.02	Análisis de impacto en el negocio	Alcance de los esfuerzos de análisis de riesgos	Interno
	DSS05.01	Evaluaciones de amenazas potenciales	Escenarios de riesgo de TI	Interno
	Fuera del Ámbito de COBIT	Avisos de amenaza	Resultados de análisis de riesgos	EDM03.03 APO01.03 APO02.02 BAI01.10
Actividades				
1. Definir la amplitud y profundidad apropiadas para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.				
2. Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta.				
3. Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.				
4. Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo.				
5. Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.				
6. Especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas. Identificar requerimientos y expectativas para los controles clave que son apropiados para las respuestas de mitigación de riesgos.				
7. Validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, confirmando que los análisis se alinean con requerimientos de empresa y verificando que las estimaciones fueron apropiadamente calibradas y examinadas ante una posible parcialidad.				

Recuperado de: (ISACA, 2019)

Tabla 20.

Práctica de Gobierno para Actividad Clave Mantener un Perfil de Riesgo

Práctica de Gestión	Entradas		Salidas	
APO12.03 Mantener un perfil de riesgo. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	De	Descripción	Descripción	A
	EDM03.01	• Niveles aprobados de tolerancia el riesgo • Guía de apetito al riesgo	Escenarios de riesgo documentados por línea de negocio y función	Interno
	APO10.04	Riesgo de entrega de proveedores identificado	Perfil de riesgo agregado, incluyendo el estado de las acciones de gestión del riesgo	EDM03.02 APO02.02
	DSS05.01	Evaluaciones de amenazas potenciales		
Actividades				
1. Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.				
2. Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.				
3. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.				
4. De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil de riesgo agregado.				
5. Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.				
6. Capturar información sobre eventos de riesgos de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.				
7. Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil de riesgo de TI de la empresa.				

Recuperado de: (ISACA, 2019)

Tabla 21.

Práctica de Gobierno para Actividad Clave Expresar el Riesgo

Práctica de Gestión	Entradas		Salidas	
APO12.04 Expresar el riesgo. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	**De**	**Descripción**	**Descripción**	**A**
			Análisis de riesgos e informes del perfil de riesgos para las partes interesadas	EDM03.03 EDM05.02 APO10.04 MEA02.08
			Revisión de resultados de evaluaciones de riesgos de terceras partes	EDM03.03 APO10.04 MEA02.01
			Oportunidades para la aceptación de un riesgo mayor	EDM03.03
Actividades				
1. Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.				
2. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.				
3. Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.				
4. Revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo. Revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales.				
5. De forma periódica, para áreas con un riesgo relativo y una paridad de capacidad del riesgo, identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.				

Recuperado de: (ISACA, 2019)

Tabla 22.

Práctica de Gobierno para Actividad Clave Definir un Portafolio de Acciones para Gestión de Riesgos

Práctica de Gestión	Entradas		Salidas	
APO12.05 Definir un portafolio de acciones para la gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	**De**	**Descripción**	**Descripción**	**A**
			Propuestas de proyecto para reducir el riesgo	APO02.02 APO13.02
Actividades				
1. Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.				
2. Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio.				
3. Definir un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.				

Recuperado de: (ISACA, 2019)

Tabla 23.

Práctica de Gobierno para Actividad Clave Responder al Riesgo

Práctica de Gestión	Entradas		Salidas	
APO12.06 Responder al riesgo. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	De	Descripción	Descripción	A
	EDM03.03	Acciones correctoras para tratar las desviaciones de gestión de riesgos	Planes de respuesta para incidentes relacionados con el riesgo	DSS02.05
			Comunicaciones del impacto del riesgo	APO01.04 APO08.04 DSS04.02
			Causas raíz relacionadas con el riesgo	DSS02.03 DSS03.01 DSS03.02 DSS04.02 MEA02.04 MEA02.07 MEA02.08
Actividades				
1. Preparar, mantener y probar planes que documenten los pasos específicos a tomar cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Asegurar que los planes incluyan vías de escalado a través de la empresa.				
2. Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.				
3. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.				
4. Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz, requerimientos de respuesta adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.				

Recuperado de: (ISACA, 2019)

Luego, la guía sugiere estándares, modelos y marcos relacionados que pueden ser utilizados para controlar el riesgo o para gestionarlo como se muestra en la tabla 24.

Tabla 24.

Guías Relacionadas para el Proceso Catalizador Gestionar el Riesgo

APO12 Guía Relacionada	
Estándar Relacionado	**Referencia Detallada**
ISO/IEC 27001:2005	Sistemas de gestión de la seguridad de información—Requerimientos, Sección 4
ISO/IEC 27002:2011	
ISO/IEC 31000	6. Procesos para la Gestión del Riesgo

Recuperado de: (ISACA, 2019)

Los mencionados controles, ya sean propios de COBIT 5 o de RISK IT se utilizarán en capítulos posteriores para sustentar la propuesta de implementación de una guía metodológica como estrategia para la gestión de riesgos del caso de estudio específico. Así también, en su trabajo de grado, (Minchala, 2016) asegura que COBIT 5 se encuentra alineado a las normas ISO 27001, 27002, 27005 y 31000.

CAPÍTULO IV

Situación Actual de la Dirección de Informática de la PUCE

Situación Actual

El presente capítulo se escribirá con información que consta en el portal de la Pontificia Universidad Católica del Ecuador (PUCE), donde existe un espacio dedicado para la Dirección de Informática y además se utilizará el documento que contiene elementos que configuran el Plan Estratégico de la Dirección de Informática alineado al Plan Estratégico de Desarrollo Institucional.

La Dirección de Informática de la PUCE es la unidad que actualmente depende de la Dirección General Administrativa y trabaja articuladamente con todas las instancias académicas y administrativas de la universidad. Su campo de acción se integra de manera transversal en colaboración a los campos de la docencia, la investigación y vinculación con la sociedad (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

La Dirección de Informática de la PUCE ofrece el diseño y desarrollo, respaldo, asesoría y acompañamiento a los proyectos administrados por las direcciones generales de la universidad y demás instancias académicas y administrativas donde se involucran las Tecnologías de la Información y Comunicación. Además, es la contraparte de proyectos tecnológicos desarrollados por externos y es la encargada de la articulación entre la sede matriz y las seis sedes de la PUCE a nivel nacional (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

En el segmento del sitio web de la PUCE, dedicado a la Dirección de Informática consta:

> La Dirección de Informática, inicialmente Centro de Cómputo, viene ofreciendo sus servicios a la comunidad universitaria desde 1977, siempre a la vanguardia

de la tecnología y apoyando su gestión en excelentes profesionales.

Somos responsables de todos los aspectos relacionados con la gestión informática de la Pontificia Universidad Católica del Ecuador, delicada y exigente misión que requiere una dedicación constante a la planificación, ejecución, control y asesoría a nuestros usuarios. (Dirección de Informática, Todos los derechos reservados 2018, pág. 1)

El área de influencia de la Dirección de informática recae sobre la comunidad universitaria (estudiantes; docentes; y, miembros del personal administrativo y de servicios) de la sede matriz y sus seis sedes en Ambato, Esmeraldas, Ibarra, Manabí, Santo Domingo de los Tsáchilas y Amazonas. A continuación, en la figura 13, se muestra un plano del campus PUCE sede matriz en Quito, la Dirección de Informática es el edificio número 28:

Figura 13.

Plano de Implantación General del Campus

Tomado de: (Planta Física PUCE, 2019)

Misión

La Dirección de Informática posee la siguiente misión:

Alineados con la misión de la PUCE, de formar íntegramente a las personas, la Dirección de Informática ofrece soluciones tecnológicas a la Comunidad Universitaria con el fin de:

- Contribuir al logro de los objetivos estratégicos y misionales de la universidad.
- Garantizar la operatividad tecnológica en la institución implementando soluciones informáticas, integrando sistemas y ofreciendo productos y servicios de alta competitividad bajo estándares de calidad a nuestros clientes internos y externos.
- Colaborar activamente en la innovación tecnológica de la universidad acompañando el desarrollo de proyectos institucionales que aporten a las funciones sustantivas.
- Velar por la renovación tecnológica y mantenimiento constante para estar alineados con las demandas de infraestructura, servicios, equipos y aplicativos, entre otros, que requieren los estudiantes y la comunidad universitaria. (Equipo de la Dirección de Informática, Todos los derechos reservados 2020, pág. 2)

Visión

La Dirección de Informática tiene la siguiente visión:

La Dirección Informática será la unidad administrativa que genera e implementa propuestas tecnológicas innovadoras, vanguardistas, orientadas a optimizar y fortalecer los procesos estratégicos en función de las necesidades institucionales incorporando recursos tecnológicos de última generación para agregar valor y competitividad a la institución en lo relacionado a docencia, investigación,

vinculación con la sociedad y gestión administrativa, sustentada por un recurso humano altamente calificado y comprometido. (Equipo de la Dirección de Informática, Todos los derechos reservados 2020, pág. 1)

Valores Institucionales

El conjunto de valores que complementados con la Visión y Misión orientan y dirigen la actividad diaria de la Dirección de Informática son:

- Privacidad: Mantenemos la seguridad de la información de la universidad, así como sus activos digitales.
- Innovación: Mantenemos un proceso de actualización y formación constante para presentar tendencias innovadoras en el desarrollo de soluciones tecnológicas.
- Colaboración: Trabajamos en equipo con todas las unidades administrativas y académicas que lo requieran, aprovechando el conocimiento y experiencia de los actores.
- Optimización: Promovemos el uso reflexivo de los recursos tecnológicos y la utilización de los equipos hasta que culmine su vida útil.
- Compromiso: Aceptación entre las partes para lograr un objetivo.
- Servicio: Basamos nuestra atención en clientes internos y externos sobre una calidad de servicio en constante mejoramiento (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

Objetivos Generales

- Dotar a la comunidad universitaria de los servicios tecnológicos, conectividad, seguridad, administración de la información, soporte técnico y la asesoría

necesaria para su correcta utilización, a través de aplicaciones informáticas, para apoyar la gestión académica, administrativa, de investigación y vinculación con la sociedad.

- Elaborar y compartir en articulación con el oficial de seguridad (DAC) las políticas, normativa y lineamientos relacionados con el uso y la aplicación de la tecnología en la matriz y todas las sedes, para garantizar la gobernanza tecnológica en la institución.
- Facilitar a todas las unidades académicas y administrativas la infraestructura tecnológica necesaria para contribuir a un trabajo eficiente en cada una de las áreas mencionadas. (Equipo de la Dirección de Informática, Todos los derechos reservados 2020, pág. 3).

Servicios que Ofrece

La Dirección de Informática de la PUCE ha puesto a disposición de la comunidad universitaria el siguiente catálogo de servicios tecnológicos que se muestra en la figura 14:

Figura 14.

Catálogo de Servicios de la Dirección de Informática de la PUCE

Tomado de: (Dirección de Informática, Todos los derechos reservados 2018)

Como se aprecia en la figura, los servicios que la Dirección de Informática ofrece corresponden a:

- Gestión de cuentas y usuarios.
- Conexión a la red haciendo posible el uso de navegación de Internet y correo electrónico.
- Servicios tecnológicos disponibles en el campus para estudiantes como impresión, préstamo de portátiles, asignación de computadores personales, etc.
- Comunicación permanente entre los miembros de la comunidad universitaria.
- Soporte de equipos, antivirus y software utilitario.
- Servicio en la nube que permite acceder a correo, guardar, sincronizar, compartir archivos y colaborar en proyectos (Dirección de Informática, Todos los derechos reservados 2018).

Estructura Organizacional

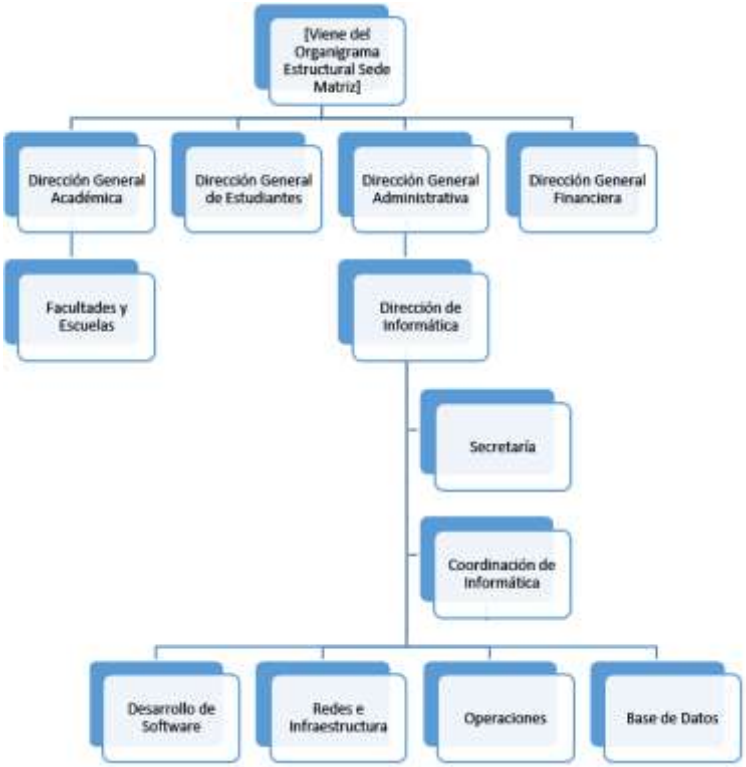
La Dirección de Informática de la PUCE, actualmente, depende de la Dirección General Administrativa y su estructura organizacional consta de cuatro áreas que

ofrecen diferentes servicios: Desarrollo de Software; Base de Datos; Redes e infraestructura y Operaciones que es la encargada de los servicios de soporte técnico y del Centro de Informática.

A Continuación, en la figura 15, se muestra un fragmento del Organigrama Estructural de la sede matriz y su correlación con la Dirección de Informática:

Figura 15.

Fragmento del Organigrama Estructural Sede Matriz y Dirección de Informática



Tomado de: (Equipo de la Dirección de Informática, Todos los derechos reservados 2020)

Áreas

Área de Desarrollo de Software

Es la unidad administrativa que, entendiendo las necesidades y requerimientos de las diferentes dependencias, analiza, diseña, desarrolla, prueba, implementa y brinda

mantenimiento a las diferentes soluciones informáticas o autoriza el desarrollo de programas, aplicativos, sistemas, sitios web, etc.; así como también el análisis e implementación de la integración de los mencionados desarrollos con los servicios que presta la institución a la comunidad universitaria. Para ello cuanta con un grupo de profesionales especialistas en tecnología informática con experiencia en el desarrollo de sistemas de información, quienes siguen los procesos y lineamientos del área para lograr software de calidad, aplicando tecnologías recientes bajo estándares establecidos internacionalmente. (Equipo de la Dirección de Informática, Todos los derechos reservados 2020, pág. 5)

Si alguna instancia administrativa requiere un desarrollo específico y justificado, deberá contactarse con el área de desarrollo de software para solicitar un proceso de análisis y luego de estudiar la factibilidad se procede al mencionado desarrollo. Si por excepción, la institución no cuenta con soluciones que se adapten y el área no pueda desarrollar la solución, alguna instancia administrativa con las respectivas justificaciones, puede adquirir el software con terceros solicitando la aprobación técnica de la Dirección de Informática desde dónde se le proporcionará la asesoría necesaria para implementar la solución, la misma que puede ser alojada dentro o fuera de la infraestructura de la institución (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

Área de Redes e Infraestructura IT

A través del Data Center institucional, el área de Redes e Infraestructura IT, es la responsable de diseñar, dimensionar, implementar, administrar y garantizar el correcto funcionamiento de la infraestructura y servicios, sea que estos se encuentren alojados en la institución o en alguna de las nubes privadas comerciales.

Es responsabilidad de esta área, que todos los servicios que la universidad ofrece desde el Data Center, sean alojados con tecnología de punta, seguridad y soporte, con el fin de garantizar un tiempo de disponibilidad alto, alineado con el software adquirido. (Equipo de la Dirección de Informática, Todos los derechos reservados 2020, pág. 6).

Los principales servicios de los que se encarga el área de Redes e Infraestructura IT son:

- Administración de cuentas de usuario para el servicio de autenticación, correo y Office 365.
- Aprovisionamiento y administración de servidores físicos y virtuales.
- Conectividad entre equipos y usuarios finales por red cableada e inalámbrica.
- Navegación segura a Internet para los usuarios internos.
- Publicación de servicios para acceso desde Internet.
- Monitoreo de la infraestructura y del acceso a servicios.
- Cableado e instalación de puntos de red (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

Área de Operaciones

El departamento de Operaciones comprende el área de Soporte Técnico y el Centro de Informática.

Soporte Técnico

Sus funciones son:

- Realizar el análisis de los requerimientos de equipos de computación solicitados por las distintas unidades y generar las especificaciones técnicas que se han definido como estándar en la universidad de acuerdo con la vanguardia tecnológica.

- Configurar los equipos de computación adquiridos por la universidad en función de las necesidades identificadas.
- Atender en Call Center para brindar soporte técnico en el transcurso de la semana laborable.
- Instalar equipos en aulas de clase de acuerdo con el equipamiento estándar y en salas de reuniones con equipo de videoconferencia.
- Gestionar el software para uso académico, en apoyo a la impartición de clases y para la plataforma estándar implementada en todo el campus.
- Realizar el mantenimiento preventivo y correctivo de estaciones de trabajo.
- Gestionar la garantía de equipos en caso de fallas (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

Centro de Informática

Cuenta con 19 aulas o laboratorios equipados con computadores y proyectores para la impartición de clases. Las aulas cuentan con software estándar, especializado y de uso libre para las carreras que lo requieran, encontrándose instalados, hasta la actualidad, más de 40 programas.

Los servicios tecnológicos implementados para estudiantes también son parte del Centro de Informática y comprenden:

- Toma de huellas y generación de credenciales para estudiantes matriculados.
- Préstamo de portátiles (control de acceso automatizado con huella digital).
- Impresión a través de quioscos instalados en el campus.
- Carga de saldo de impresión a través de tarjeta de recarga.
- Servicio express a través de quioscos para uso del personal de servicios generales y para estudiantes (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

Área de Base de Datos

El área de Base de Datos es la encargada de administrar, supervisar y asegurar el uso adecuado de los datos del Database Management System (DBMS). Esta área administra las bases de datos de los sistemas que permiten manejar la data de una manera eficiente. Dos de sus campos principales de acción son:

- La administración de los datos que proporciona estándares, guías de acción, procedimientos de control y la documentación necesaria para garantizar que los usuarios trabajen en forma cooperativa y complementaria al procesar la información.
- La administración de la Base de Datos propiamente dicha relacionada al control y supervisión de los procesos realizados en los gestores de bases de datos, a fin de garantizar la disponibilidad continua de este recurso imprescindible para la institución.

Entre los aspectos más importantes del trabajo del área de Base de Datos están el proteger los datos de la institución, lo que incluye hacer copias de seguridad periódicas de los datos y mantenerlos a salvo de la destrucción accidental o intencional. Además, diseñar, implementar y probar un plan de recuperación de los mismos (Equipo de la Dirección de Informática, Todos los derechos reservados 2020).

Análisis FODA

A continuación, se muestra el análisis de fortalezas, oportunidades, debilidades y amenazas, nótese que, entre las debilidades, sobre el trabajo interno de la Dirección de Informática, se destacan:

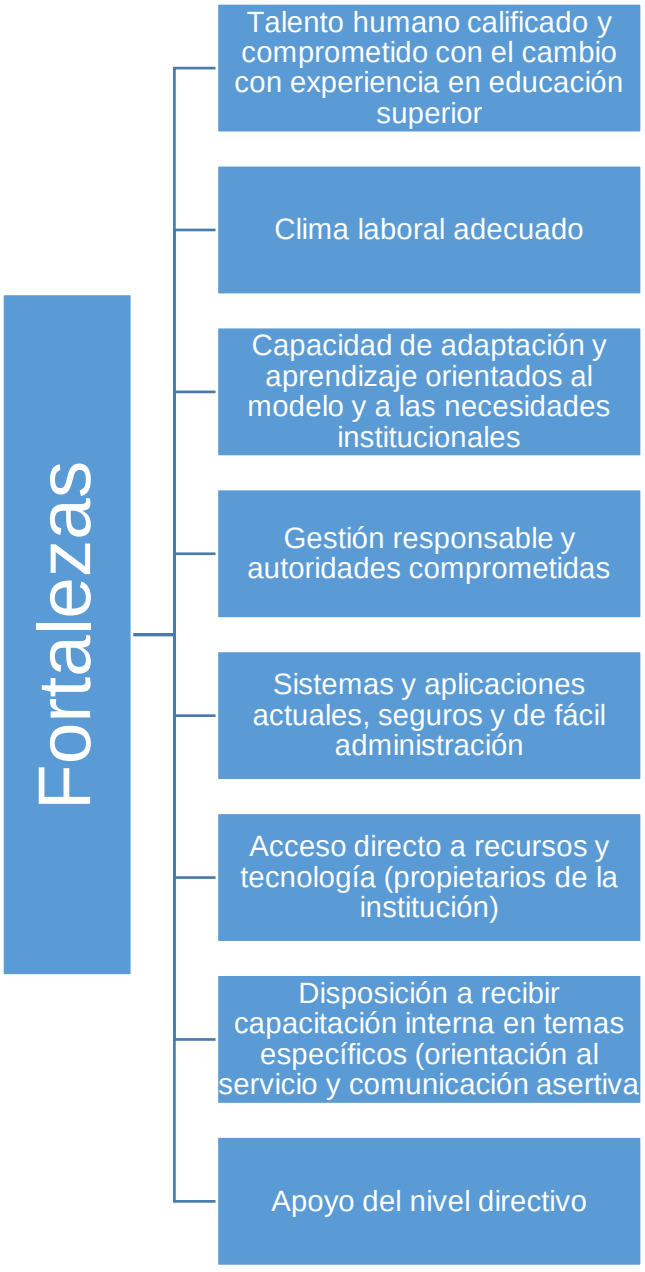
- Carencia de documentos sobre Políticas de Gobierno de TI.
- Políticas y procedimientos no actualizados.

- Análisis de riesgos insuficiente.

Razones que, en primera instancia, motivaron el presente estudio basado en RISK IT como estrategia de gestión de riesgos.

Figura 16.

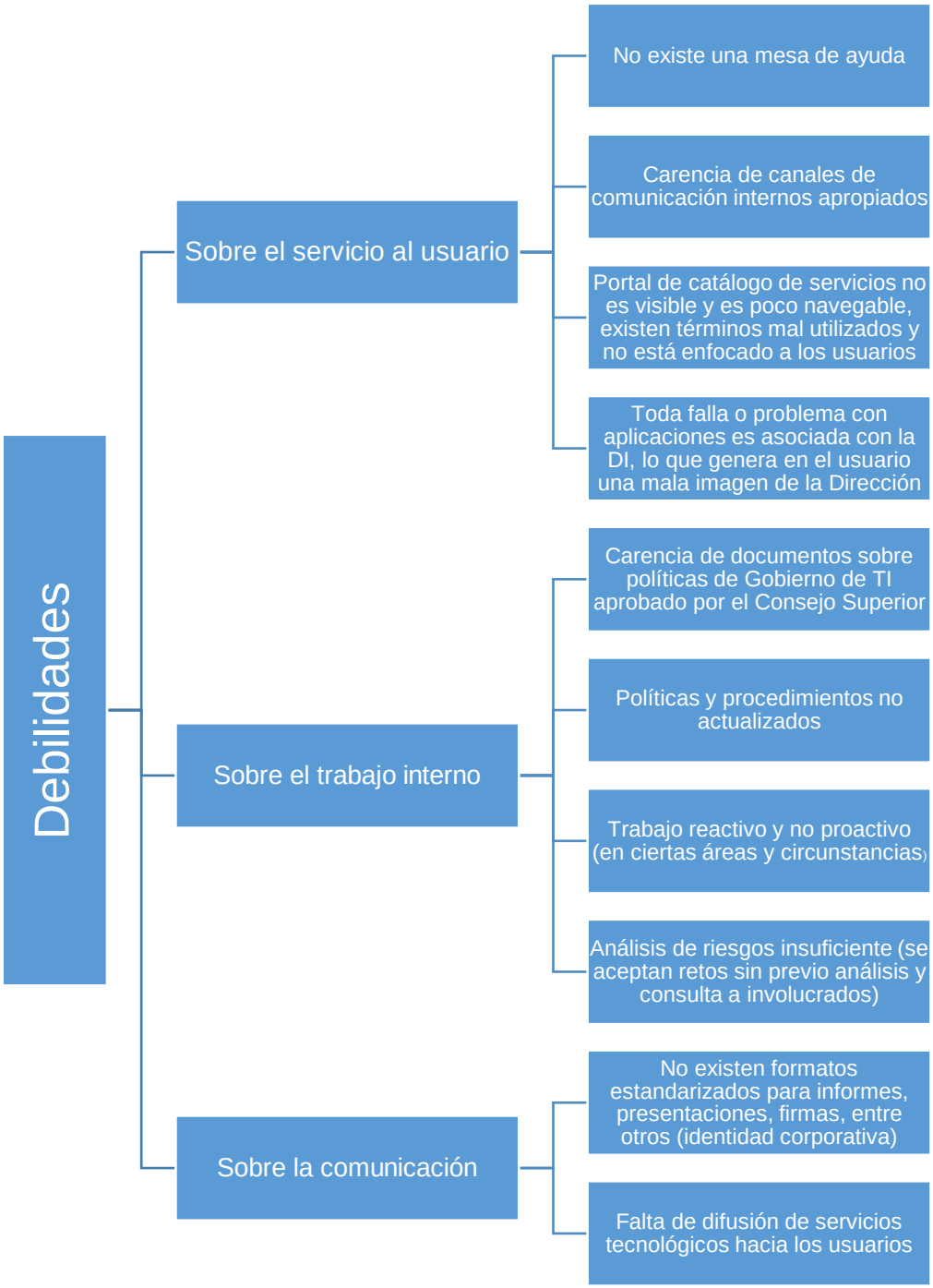
Análisis de Fortalezas de la Dirección de Informática



Tomado de: (Equipo de la Dirección de Informática, Todos los derechos reservados 2020)

Figura 17.

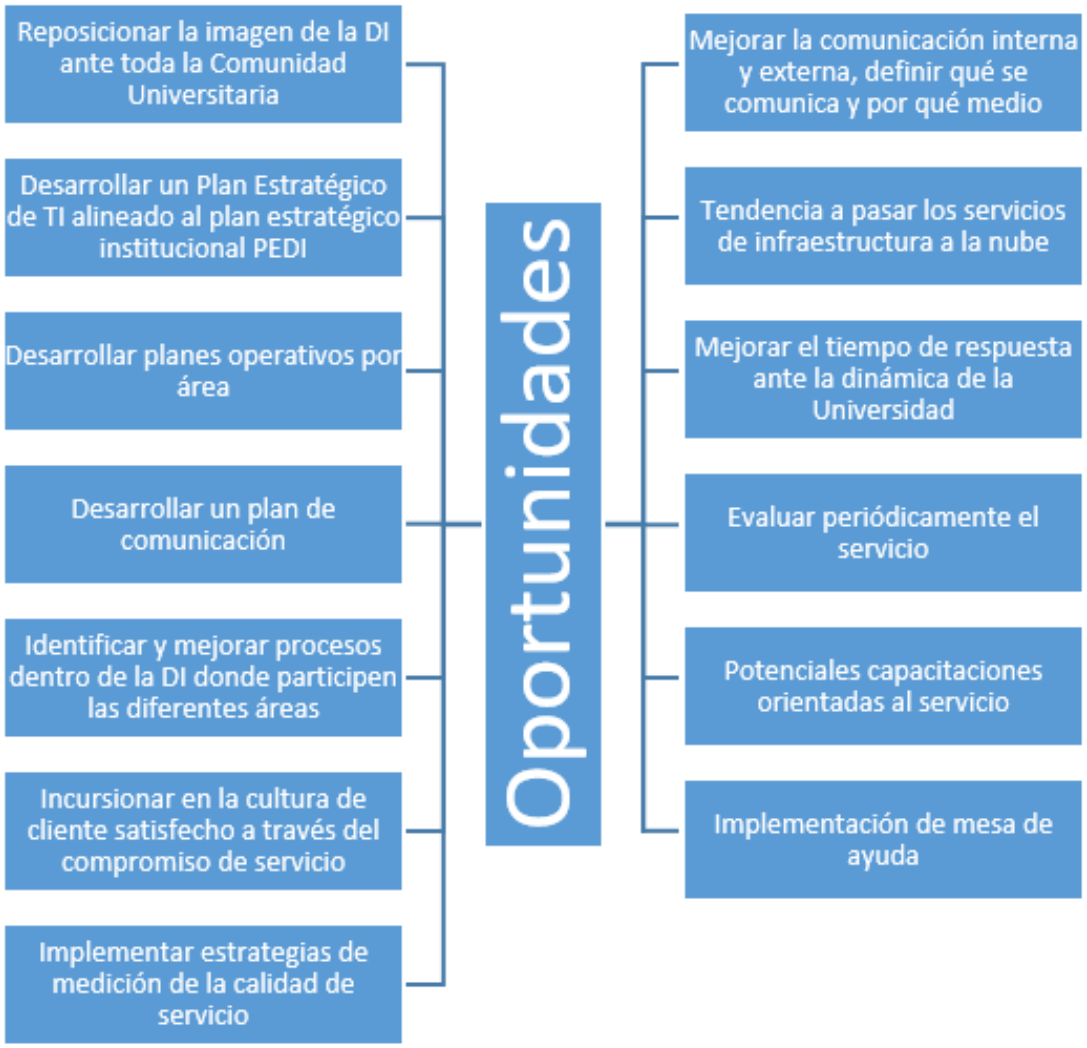
Análisis de Debilidades de la Dirección de Informática



Tomado de: (Equipo de la Dirección de Informática, Todos los derechos reservados 2020)

Figura 18.

Análisis de Oportunidades de la Dirección de Informática



Tomado de: (Equipo de la Dirección de Informática, Todos los derechos reservados 2020)

Figura 19.

Análisis de Amenazas de la Dirección de Informática

Tomado de: (Equipo de la Dirección de Informática, Todos los derechos reservados 2020)

CAPÍTULO V

Propuesta de Implementación de una Guía Metodológica Basado en RISK IT para la Gestión de Riesgos en la Dirección de Informática de la Pontificia Universidad Católica del Ecuador - PUCE

Información Preliminar

Ruta de Investigación

Dado que el presente capítulo implica una propuesta de implementación de una guía metodológica, es propicio escoger una ruta de investigación adecuada que sustente el procedimiento metodológico general con el cual se abordará el problema de investigación planteado inicialmente.

Entonces, para cumplir con el propósito mencionado, se escribirá en primera instancia, un marco metodológico que es un conjunto de pasos que conducen a solucionar una situación; el mismo que debe describir los procedimientos que incluyen la técnica para solventar el cómo se realizará la resolución del problema de investigación (Hernández & Mendoza, Metodología de la Investigación, 2018). En segundo lugar, se documentará el desarrollo del componente técnico para el presente trabajo de titulación con el apoyo de la herramienta RISK IT para gestión de riesgos.

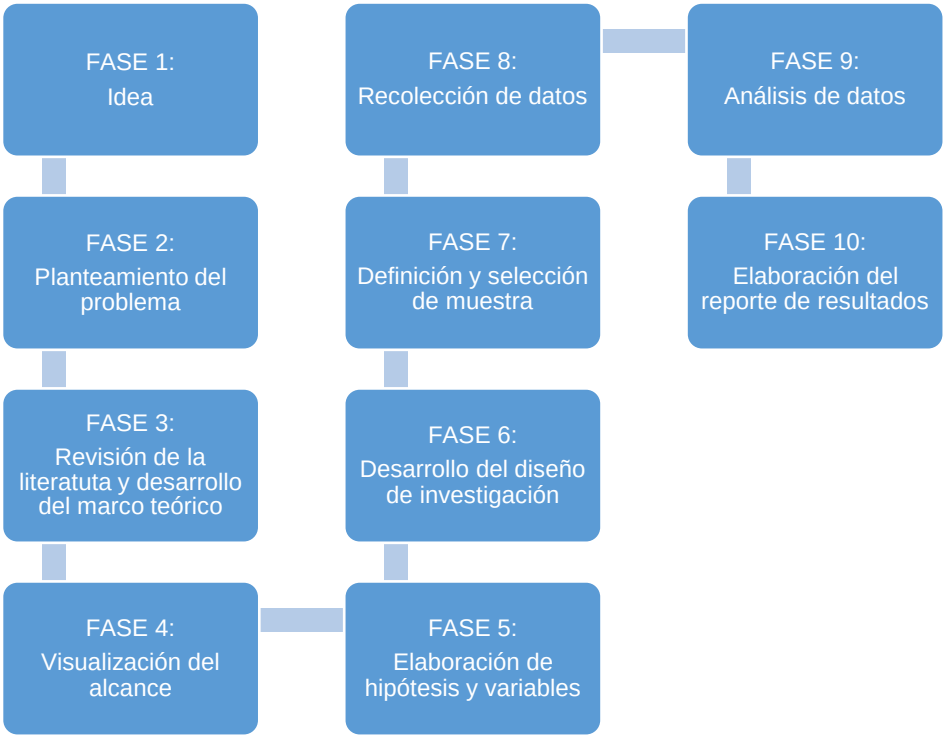
Ruta de Investigación Cuantitativa

Según los autores Hernández y Mendoza (2018), la investigación cuantitativa se vincula a conteos numéricos y métodos matemáticos organizados de manera secuencial. Cada fase precede a la siguiente en orden riguroso, pudiéndose redefinir alguna etapa. Se parte de una idea; se generan objetivos y preguntas de investigación; se revisa la literatura disponible construyéndose la perspectiva teórica.

De las preguntas deberán desprenderse hipótesis que para ser operacional izadas definen variables; se seleccionan casos para, en estos, medir las variables en un contexto específico; se analizan las mediciones utilizando métodos estandarizados y se concluye sobre las hipótesis, siendo un proceso como se representa en la figura 20 (Hernández & Mendoza, Metodología de la Investigación, 2018):

Figura 20.

Proceso de Investigación Cuantitativo



Tomado de: (Hernández & Mendoza, Metodología de la Investigación, 2018)

Las características relevantes de la ruta de investigación cuantitativa son:

1. Los datos se encuentran en forma de números y su recolección se fundamenta en la medición.
2. Se busca mayor objetividad en todo el proceso o ruta.

3. Se sigue un patrón predecible y estructurado donde los datos poseen estándares de validez y confiabilidad deseados, y las conclusiones derivadas contribuyen a la generación de conocimiento.
4. Se vale de la lógica deductiva, es decir, parte de lo general a lo particular.
5. Se busca conocer o capturar el fenómeno estudiado tal como es o aproximarse lo mejor posible a él. Las suposiciones deben ajustarse a dicha realidad y no al revés (Hernández & Mendoza, Metodología de la Investigación, 2018).

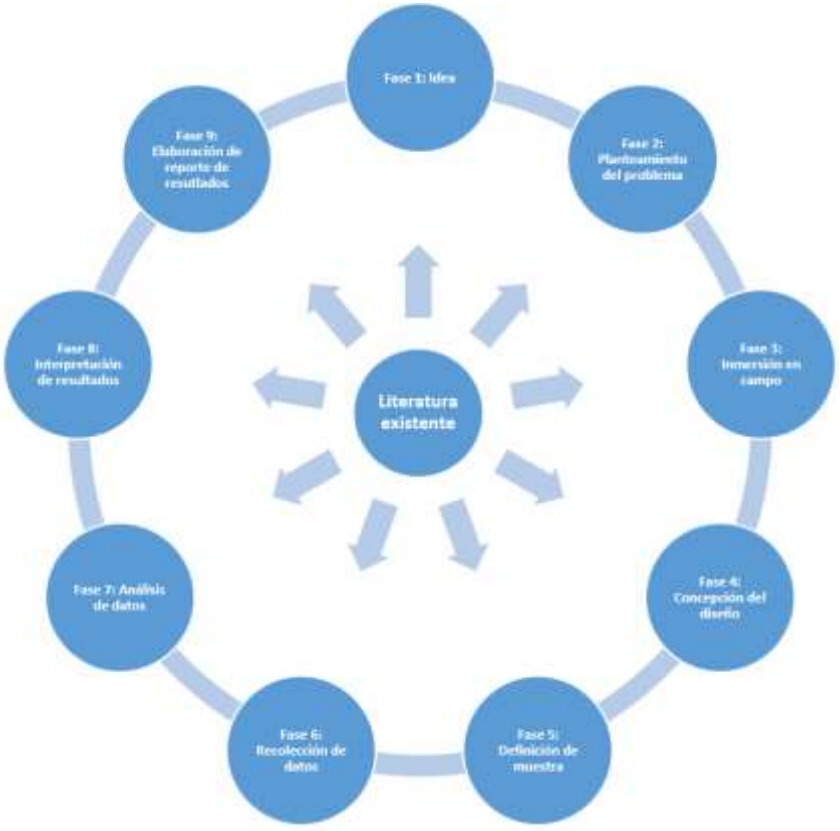
Ruta de Investigación Cualitativa

En el enfoque cualitativo también se estudian fenómenos de manera sistemática. Sin embargo, en lugar de comenzar con una teoría y luego confirmar si está apoyada por los datos y los resultados, se examinan los hechos en sí y se revisan estudios previos simultáneamente, para generar una teoría consistente con lo que se está observando que sucede.

El problema de investigación se enfoca paulatinamente de acuerdo al contexto. La acción indagatoria es dinámica entre los hechos y su interpretación siendo un proceso más flexible al caso de estudio, representado en la figura 21 (Hernández & Mendoza, Metodología de la Investigación, 2018):

Figura 21.

Proceso de Investigación Cualitativo



Tomado de: (Hernández & Mendoza, Metodología de la Investigación, 2018)

Las características relevantes de la ruta de investigación cualitativa son:

1. La revisión de literatura puede complementarse en cualquier etapa del estudio desde el planteamiento del problema hasta la elaboración del reporte de resultados.
2. La investigación de campo implica sensibilizarse con el entorno en el que se llevará a cabo el estudio y se identifica a los informantes que aportan los datos para que guíen al investigador.
3. La recolección de datos y su análisis se hace casi simultáneamente o van influyéndose mutuamente.

4. El enfoque cualitativo resulta conveniente para comprender fenómenos desde la perspectiva de quienes los experimentan y cuando se buscan patrones o diferencias en esas experiencias.
5. Se vale, en mayor medida del razonamiento inductivo, dirigiéndose de lo particular a lo general.
6. Su propósito es reconstruir la realidad tal como la observan los actores, siendo holístico, porque se precia de considerar el todo sin reducirlo al estudio de sus partes.
7. Los métodos de recolección de datos no son estandarizados ni completamente predeterminados. Las técnicas se utilizan con flexibilidad y de acuerdo con el estudio podrían ser entrevistas, observación, revisión de documentos, grupos de enfoque, etc.
8. Los resultados no pretenden generalizar de manera probabilística a otras muestras sino que pretenden que se sitúen y contextualicen los descubrimientos (Hernández & Mendoza, Metodología de la Investigación, 2018).

Ruta de Investigación Mixta

Es el enfoque de investigación que se utilizará en el presente trabajo de titulación. Esta ruta de investigación entrelaza y mezcla a las dos anteriores, no sólo las suma, sino que realiza una interacción para potencializarlas. Los métodos mixtos o híbridos representan un conjunto de procesos sistemáticos, empáticos y críticos de investigación e implican el análisis de datos cuantitativos y cualitativos, su integración y discusión para lograr inferencias y un mayor entendimiento de la realidad. Los métodos mixtos pueden implementarse de acuerdo a distintas secuencias.

A veces, lo cuantitativo precede a lo cualitativo y otras veces lo cualitativo es primero; pero también, pueden desarrollarse de manera paralela o se pueden fusionar a

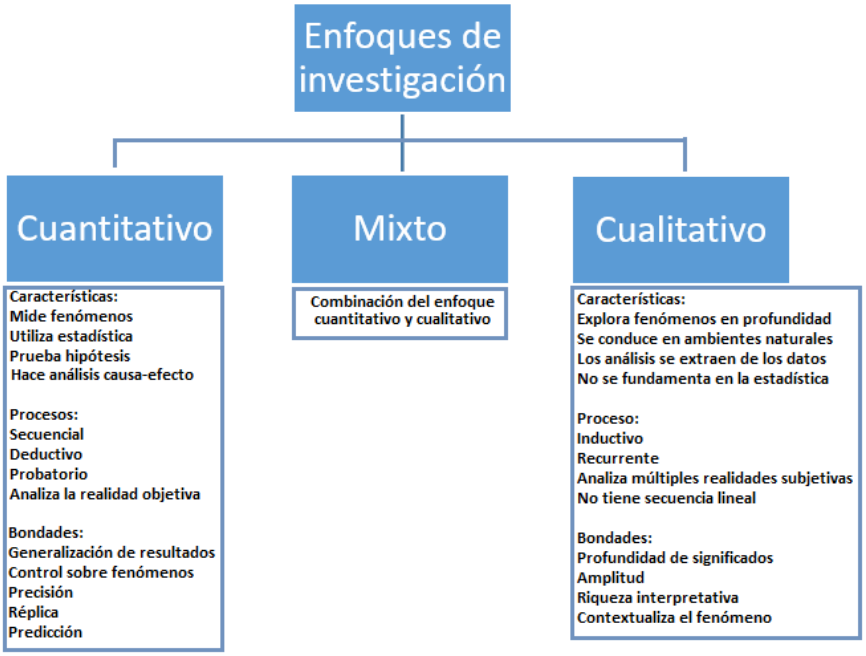
lo largo de la investigación (Hernández & Mendoza, Metodología de la Investigación, 2018). Las características relevantes de la ruta de investigación mixta son:

1. Provee una perspectiva más amplia y profunda del tema de investigación.
2. Permite una mayor teorización.
3. Recaba datos variados y posibilita una mejor exploración y explotación de los mismos.
4. Concede una indagación más dinámica que en otros métodos.
5. Asigna una mayor solidez y rigor (Hernández & Mendoza, Metodología de la Investigación, 2018).

A continuación, en la figura 22, se presentan las características, una reseña del proceso y las bondades de los enfoques antes descritos y dónde se encuentra la ruta de investigación mixta:

Figura 22.

Enfoques de la Investigación y Proceso de Investigación Mixto



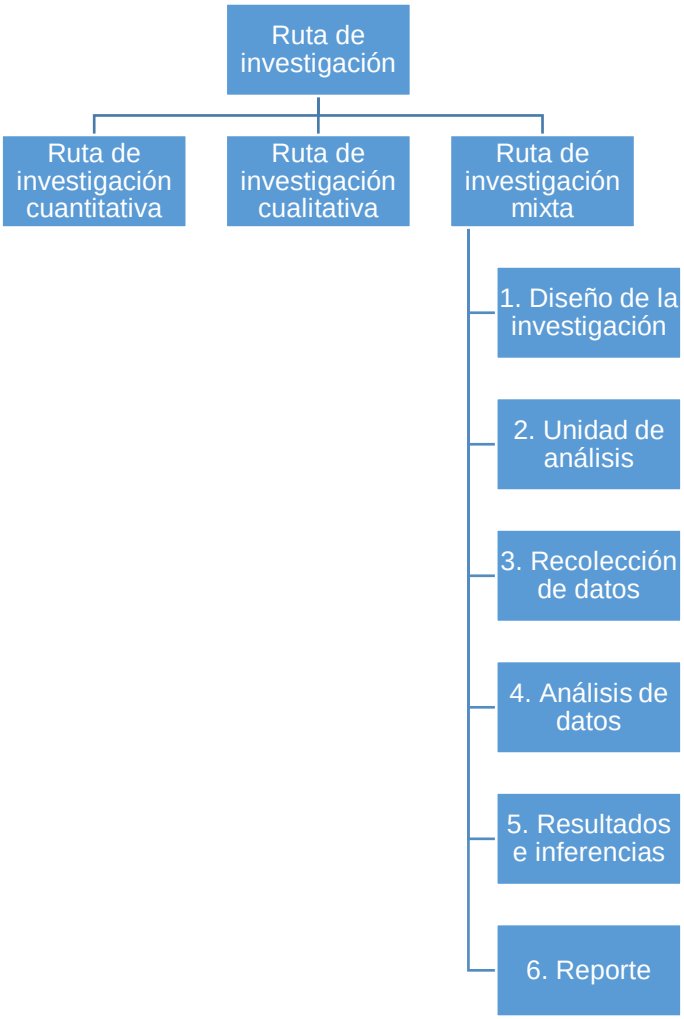
Tomado de: (Hernández, Fernández, & Baptista, Metodología de la Investigación, 2010)

Tal como se explicó anteriormente, se decidió aplicar para la presente investigación, una ruta de métodos mixtos cuya meta no es reemplazar a la investigación cuantitativa ni a la investigación cualitativa, sino utilizar las fortalezas de ambos tipos de indagación, combinándolas.

En la figura 23 constan los pasos que describen el proceso para el caso de estudio:

Figura 23.

Ruta Mixta Diseñada como Metodología General de Investigación



Tomado de: (Hernández, Fernández, & Baptista, Metodología de la Investigación, 2010)

En los siguientes numerales se procederá a describir cada una de las fases de esta metodología general de investigación escogida:

1. **Diseño de la Investigación:**

En la obra de los autores Hernández y Mendoza (2018), se señala que realmente no existe un proceso mixto único. En un estudio mixto o híbrido concurren diversos procesos. Para el diseño de la investigación, un estudio mixto comienza con un planteamiento de la problemática que demanda la integración de los enfoques cuantitativo y cualitativo. La formulación del planteamiento tiene tres momentos:

- Al inicio del estudio, producto de una primera evaluación del problema y además revisión de la literatura.
- Durante el estudio, al momento de tomar decisiones sobre los métodos.
- Una vez que se tienen los primeros resultados, al momento de realizar interpretaciones emergentes (Hernández & Mendoza, Metodología de la Investigación, 2018).

Después del planteamiento de la problemática vendrá la revisión de la literatura pertinente, de la misma forma que se realiza en la investigación cuantitativa y cualitativa. Consecuentemente, se elaborará un marco teórico que se fundamenta en marcos de referencia, teorías o perspectivas para la realización del estudio.

Luego de la revisión de la literatura y su respectivo sustento teórico se diseñará la investigación propiamente dicha. Uno de los diseños que se ajusta al presente trabajo de titulación y que es considerado un diseño mixto es el diseño de investigación – acción.

Diseño de Investigación – Acción:

Su finalidad es comprender y resolver problemáticas específicas de una colectividad vinculadas a un ambiente, organización o grupo. Además, se centra en aportar información que guíe la toma de decisiones para algún proceso.

La investigación – acción pretende transformar la realidad y que las personas tomen conciencia de su papel en ese proceso de transformación. Por tal razón, implica la colaboración de los participantes en la detección de necesidades, el involucramiento con la estructura a modificar, el proceso a mejorar, las prácticas que requieren cambiarse y la implementación de los resultados del estudio. Los autores ubican a la investigación – acción en los marcos referenciales interpretativo y crítico. Se abarcan tres fases:

1. Observar: Construir el bosquejo del problema y recolectar datos.
2. Pensar: Analizar e interpretar.
3. Actuar: Resolver la problemática e implementar mejoras.

Algunos de los instrumentos que se pueden utilizar para cumplir con esas fases en sus primeras etapas son entrevistas, observaciones en el ambiente, actividades que se relacionan con la problemática, grupos de enfoque, revisión de documentos, registros y materiales pertinentes. Incluso algunos instrumentos serán de carácter cuantitativo como estadística. En lo que respecta al análisis se pueden utilizar mapas conceptuales, diagramas causa – efecto, matrices de categorías, organigramas de estructura formal. Finalmente, se realiza el reporte con un diagnóstico de la problemática y se lo socializa con los participantes para validar la información y confirmar los hallazgos (Hernández & Mendoza, Metodología de la Investigación, 2018).

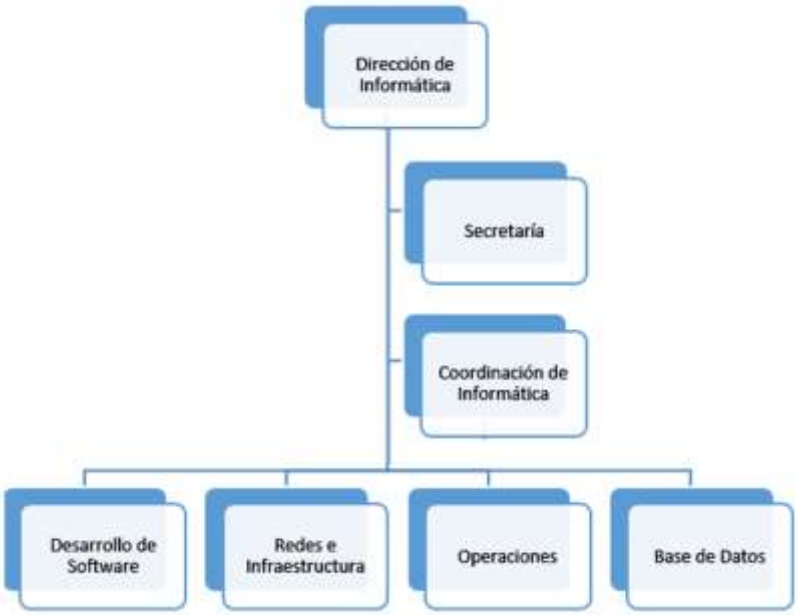
2. Unidad de Análisis:

Plantea seleccionar una población de interés, un área de influencia, un objeto, varios procesos, grupos o comunidades, una unidad de estudio, etc., que se beneficiarán con el análisis para recolectar datos necesarios a fin de responder al planteamiento del problema de investigación.

La unidad de análisis del presente trabajo de titulación es la Dirección de Informática de la PUCE y las áreas que la conforman como se puede visualizar en la figura 24:

Figura 24.

Organigrama Estructural de la Dirección de Informática



Tomado de: (Equipo de la Dirección de Informática, Todos los derechos reservados 2020)

3. Recolección de Datos:

La obra de Hernández y Mendoza (2018), recomienda al investigador decidir sobre los tipos específicos de datos que se han de recolectar. Los lineamientos para la recolección de datos y el análisis pertinente en la ruta mixta son:

- Tanto predeterminados como emergentes.
- Tanto estandarizados como no estandarizados.
- Empíricos, tanto medibles u observables como inferidos.
- Categorías de diferente naturaleza y mezcla de estas.
- Formas múltiples de datos obtenidos de todas las posibilidades.

- Resumidos en matrices de datos numéricos y datos convertidos, así como bases de datos y de texto e información combinada.
- Interpretativos a través de cruzar y/o mezclar las bases de datos.

Gracias al desarrollo de los métodos mixtos y la nueva posibilidad de hacer compatibles los programas de análisis cuantitativo y cualitativo, unas variedades de datos recolectados pueden ser tabulados y codificados como números y como texto, o ser transformados de cuantitativos a cualitativos y viceversa (Hernández & Mendoza, Metodología de la Investigación, 2018).

La elección del tipo de instrumento y el tipo de datos a recolectar dependerá del planteamiento de la investigación.

La recolección de datos para el caso de la Dirección de Informática de la PUCE se mostrará más adelante como parte de la propuesta de implementación de una guía metodológica basado en RISK IT.

4. **Análisis de Datos:**

En los métodos mixtos el investigador confía en los procedimientos estandarizados y cuantitativos, así como en los cualitativos, además de análisis combinados. La selección de técnicas y modelos de análisis también se relaciona con el planteamiento del problema, el diseño de la investigación y puede realizarse sobre los datos directos u originales o puede requerir de su transformación (Hernández & Mendoza, Metodología de la Investigación, 2018).

El análisis de datos para el caso de la Dirección de Informática de la PUCE se mostrará más adelante como parte de la propuesta de implementación de una guía metodológica basado en RISK IT.

5. **Resultados e Inferencias:**

Una vez que se obtienen los resultados del análisis cuantitativo, cualitativo o mixto se procede a desarrollar inferencias, comentarios y conclusiones. Normalmente,

se tienen tres tipos de inferencias: las propiamente cuantitativas, las cualitativas y las mixtas; a estas últimas se las llama metainferencias.

A las inferencias se las presenta en el reporte de algunas maneras: podrán ser primero las pertenecientes a cada método y luego las conjuntas; o por áreas de resultados de las tres clases de inferencias. En el primer caso (las pertenecientes a cada método y luego las conjuntas), el orden puede depender del peso de cada enfoque y en el segundo caso (por áreas de resultados), el orden puede estar sujeto por la secuencia de las preguntas de investigación o por la importancia de los hallazgos (Hernández & Mendoza, Metodología de la Investigación, 2018).

Los resultados e inferencias para el caso de la Dirección de Informática de la PUCE se mostrarán más adelante como parte de la propuesta de implementación de una guía metodológica basado en RISK IT.

6. **Reporte:**

Para la presentación del reporte se han generado algunas directrices:

- El reporte debe abarcar tanto la investigación cuantitativa como la cualitativa, deben incluirse ambas aproximaciones y tanto en la recolección de datos, análisis e integración de los mismos, así como las inferencias derivadas de los resultados.
- Los estudios mixtos son más que reportar las dos ramas de indagación cuantitativa y cualitativa; deben vincularlas y conectarlas analíticamente.
- El informe mixto incluye componentes de ambos métodos que cubran vacíos en el conocimiento y agreguen nuevas perspectivas a la literatura sobre la investigación mixta (Hernández & Mendoza, Metodología de la Investigación, 2018).

El reporte para el caso de la Dirección de Informática de la PUCE se mostrará más adelante como parte de la propuesta de implementación de una guía metodológica basado en RISK IT plasmado en un documento de la propuesta de implementación.

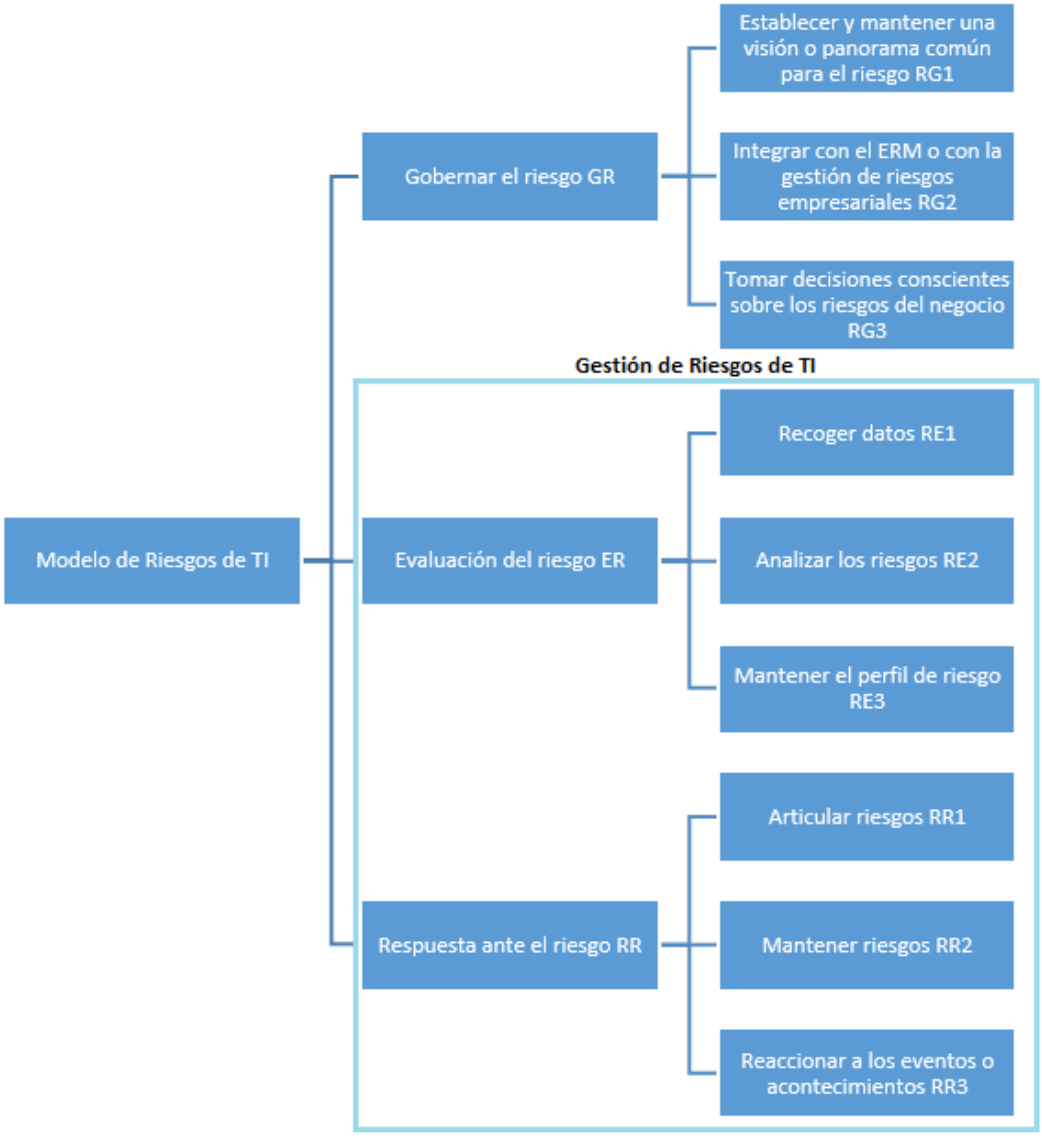
Propuesta de Implementación de una Guía Metodológica Basado en RISK IT para la Dirección de Informática de la PUCE

Una vez escrita la metodología general de investigación se procede a abordar el área técnica, las dos: metodología general y área técnica poseen coherencia entre ellas y son complementarias.

Anteriormente, se había documentado sobre lo que RISK IT propone como un modelo para la gestión de riesgos de TI. Este marco se divide en tres ámbitos o dominios y cada uno contiene tres procesos:

Figura 25.

Modelo de Riesgos de TI como Metodología Propuesta por RISK IT



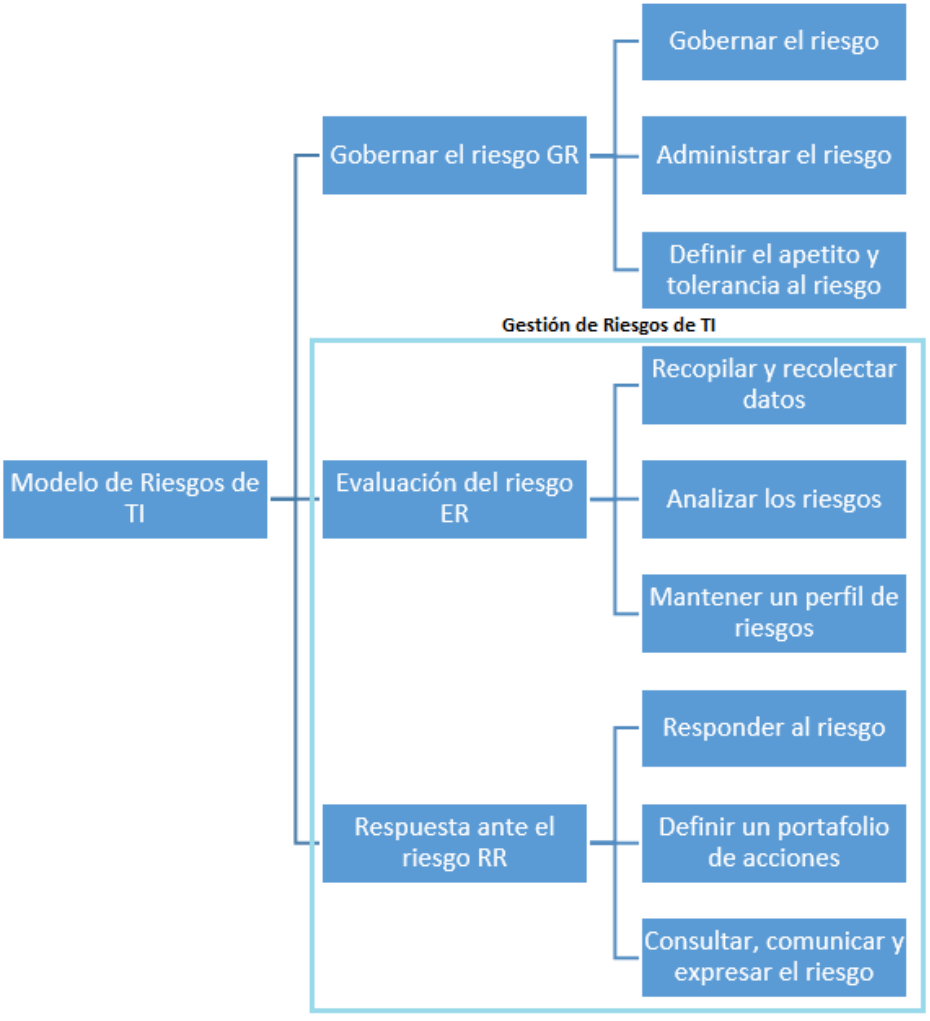
Tomado de: (ISACA, 2020)

Con lo anteriormente expresado, en la presente sección se abordará la propuesta de implementación de una guía metodológica para gestionar riesgos para el caso específico de la Dirección de Informática de la PUCE guardando congruencia con lo planteado por la herramienta RISK IT de ISACA que se mostró en la figura 25.

De la literatura revisada en libros digitales, artículos, tesis de grado, y además en el Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa de COBIT 5; en el Marco de Gestión de Riesgos de TI; en la Guía de Procesos Catalizadores y en la Guía Profesional de RISK IT se ha podido generar lo siguiente como metodología propuesta:

Figura 26.

Marco o Modelo de Riesgos de TI como Metodología Propuesta



En la figura 26 se muestra la metodología propuesta para gestión de riesgos para la Dirección de Informática de la PUCE. A continuación, se describirá cada paso de la metodología y se hará referencia al Anexo Único donde se escribirá la propuesta de implementación de una guía metodológica para el caso específico mencionado.

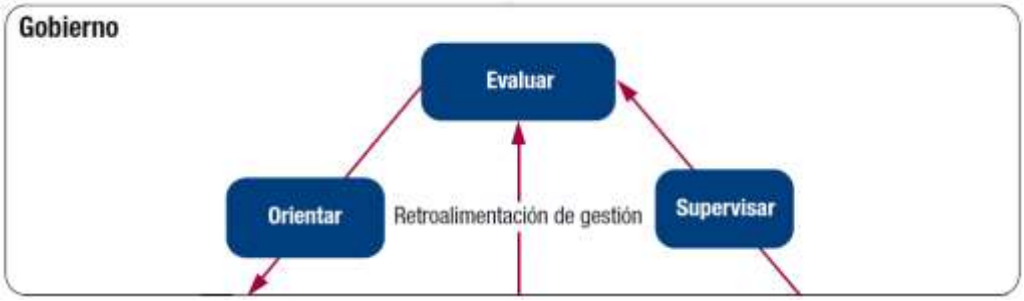
Paso 1. Gobernar el Riesgo:

"El término gobernar ha pasado a estar a la vanguardia del pensamiento empresarial como respuesta a algunos hechos que han demostrado la importancia de un buen gobierno" (Chambi, 2018, pág. 78). Se debe gobernar de forma integral, es decir, cubriendo la empresa extremo a extremo como se enfatiza en el segundo principio de COBIT 5 (ISACA, 2012) procurando la creación de valor que es una de las asignaciones de los cargos de gobierno de la empresa, orientando este esfuerzo hacia satisfacer las necesidades de las partes interesadas. Adicionalmente, en COBIT 5 se indica que es necesario diferenciar las actividades delegadas al gobierno de la empresa de las que le corresponden a la administración, siendo este el quinto principio que rige la filosofía COBIT 5 (ISACA, 2012).

La herramienta RISK IT indica que el éxito del gobierno corporativo radica en que existen grados o niveles de uso estratégico que se les puede dar a las TIC y que estas apalancan los recursos de la empresa para reducir el riesgo global, pero para ello se necesitan políticas y estas deben partir de la dirección o gobierno empresarial. Con lo cual, el punto de partida para iniciar el proceso de gestión de riesgos de TI debe ser contar con políticas para todas las dimensiones de la empresa que son generadas desde el ámbito de gobierno que se encarga de evaluar, orientar y supervisar, tal como lo muestra el modelo de referencia en la porción superior de la pirámide organizacional (ISACA, 2020) y que se puede observar en la figura 27:

Figura 27.

Áreas Clave de Gobierno de COBIT 5



Tomado de: (ISACA, 2012)

Cuando se mencionan los procesos de TI empresarial en las áreas citadas: evaluar, orientar y supervisar, se debe tener en consideración el proceso EDM03 que es Asegurar la Optimización del Riesgo, tal como lo indica el modelo de referencia sobre procesos COBIT 5 (ISACA, 2012), siendo el único proceso referente a riesgos del que se debe encargar el gobierno de TI empresarial:

Figura 28.

Procesos para Gobierno de la TI Empresarial de COBIT 5

Tomado de: (ISACA, 2012)

Para el caso de la Dirección de Informática de la PUCE la responsabilidad de gobernar el riesgo debe recaer sobre el rol consignado específicamente para realizar esta actividad, RISK IT propone varias figuras como el Director Ejecutivo (Chief Executive Officer CEO, que es el más alto rango que se encarga de la gestión de la organización); el Director de Riesgo (Chief Risk Officer CRO, que supervisa los

aspectos de gestión de riesgos de la organización), y; el Responsable de Información (Chief Information Officer CIO, que es el responsable de las tecnologías de la información). Con cualquier denominación, este cargo debe asegurar que la actividad de gestión de riesgos se alinea con la capacidad objetiva de la empresa y el liderazgo de la misma según lo que indican las pautas de RISK IT.

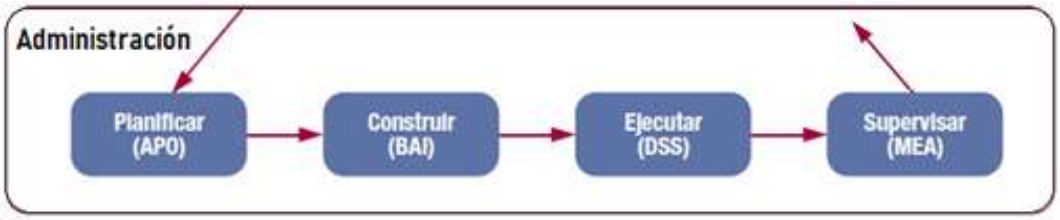
Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 2. Administrar el Riesgo:

Como se mencionó en el segundo capítulo del presente trabajo de titulación, administrar es distinto que gestionar, administrar es una instancia previa, implica utilizar los recursos disponibles en la empresa para planificar acciones que ayuden a conseguir los objetivos planteados, en cambio; gestionar es poner en marcha lo planificado durante la administración. En las organizaciones, la administración es responsabilidad de los ejecutivos a cargo del Director General (CEO). Las áreas de responsabilidad son planificar, construir, ejecutar y supervisar como lo muestra el modelo de referencia en la porción inferior de la pirámide organizacional (ISACA, 2020) y que se puede observar en la figura 29:

Figura 29.

Áreas Clave de la Administración de COBIT 5

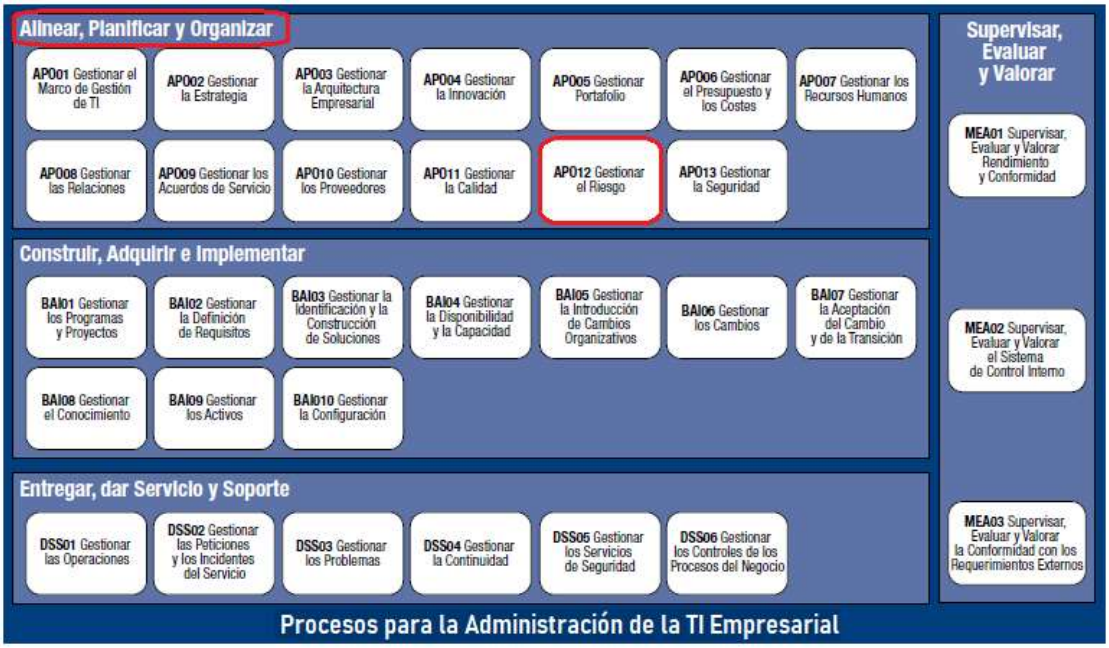


Tomado de: (ISACA, 2012)

Cuando se mencionan los procesos de TI empresarial en las áreas citadas: planificar, construir, ejecutar y supervisar, se debe tener en consideración el proceso APO12 que es Gestionar el Riesgo, tal como lo indica el modelo de referencia sobre procesos COBIT 5 (ISACA, 2012), siendo el único proceso referente a riesgos del que se debe encargar la administración de TI empresarial y que pertenece al área de Alinear, Planificar y Organizar:

Figura 30.

Procesos para la Administración de la TI Empresarial de COBIT 5



Tomado de: (ISACA, 2012)

Para el caso específico de la Dirección de Informática de la PUCE la responsabilidad de administrar el riesgo recae sobre el rol consignado específicamente a realizar esta actividad, RISK IT propone la figura del Comité de Riesgos (conformado por los ejecutivos que son los responsables de las áreas de la empresa para apoyar las actividades de gestión de riesgos). Con cualquier denominación, estos responsables

deben integrar la estrategia de riesgos de TI y operaciones con la estrategia de riesgo del negocio según lo que indican los lineamientos de RISK IT (ISACA, 2020).

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 3. Definir el Apetito y la Tolerancia al Riesgo:

Para el autor Jaramillo (2013) el apetito al riesgo es la cantidad de riesgo que una entidad está dispuesta a aceptar para cumplir su misión y visión. Al examinar los niveles de apetito para una organización, surgen dos factores: la capacidad objetiva de la organización para absorber una pérdida y la predisposición a asumir riesgos prudentes o agresivos, es decir que en la organización exista una cultura de riesgos.

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

En el tercer capítulo del presente trabajo de titulación, se mostró teoría sobre bandas para los mapas de riesgos, delimitadas por colores, según el nivel de apetito al riesgo definido en la cultura de riesgos de cada organización (ISACA, 2020). La recomendación se tomó del Marco de Gestión de Riesgos de TI (RISK IT Framework) y se ha planteado como sugerencia para el caso específico del presente trabajo de titulación.

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

En resumen, el apetito al riesgo indica la magnitud de riesgo que la organización está dispuesta a afrontar para alcanzar una meta y la tolerancia indica hasta dónde se

podría aceptar una variación de esa magnitud para conseguir la misma meta después de haber sucedido un evento riesgoso.

Según las pautas de RISK IT, realizar definiciones sobre el apetito y tolerancia al riesgo es asegurar que las decisiones concretas de la organización consideren la gama de oportunidades y las consecuencias de la dependencia a las TI para el éxito de la organización (ISACA, 2020).

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 4. Recopilar y Recolectar Datos:

Realizados los pasos anteriores se procede a identificar los datos pertinentes para hacer visible la identificación de riesgos de TI. Se parte de la identificación de activos:

Identificar los Activos de Información:

En la investigación de Crespo (2016) se indica que el activo de información hace referencia a cualquier elemento que contenga información. El autor plantea los siguientes grupos de clasificación de activos de información (Crespo, 2016):

Figura 31.

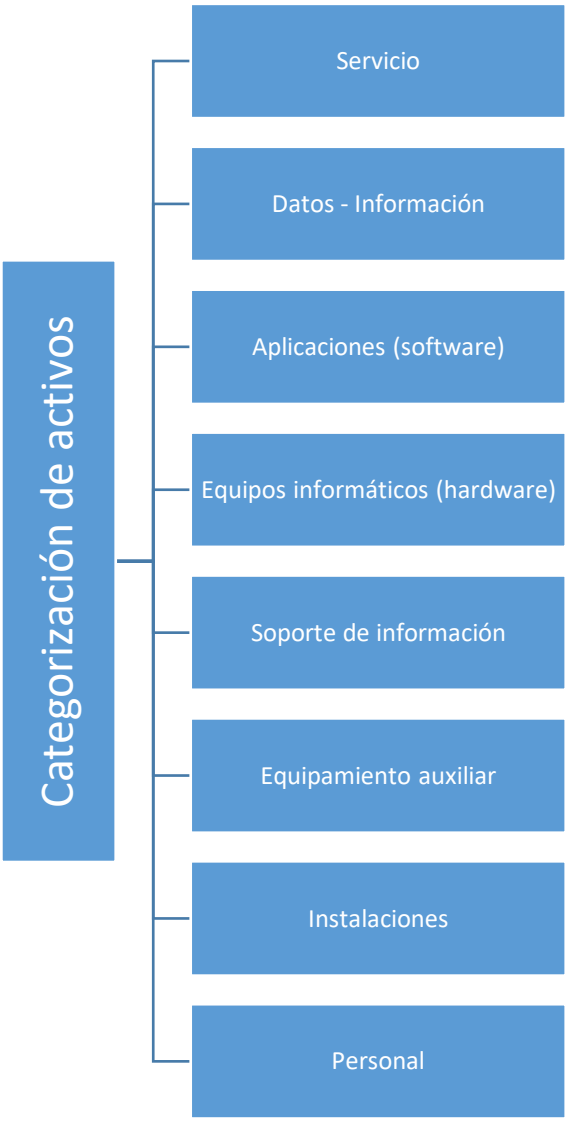
Clasificación de Activos de Información. Ejemplo 1

Tomado de: (Crespo, 2016)

Por otro lado, los autores Cruces y Mora (2016) en su obra, clasifican a los activos de la siguiente manera (Cruces & Mora, 2016):

Figura 32.

Categorización de Activos. Ejemplo 2

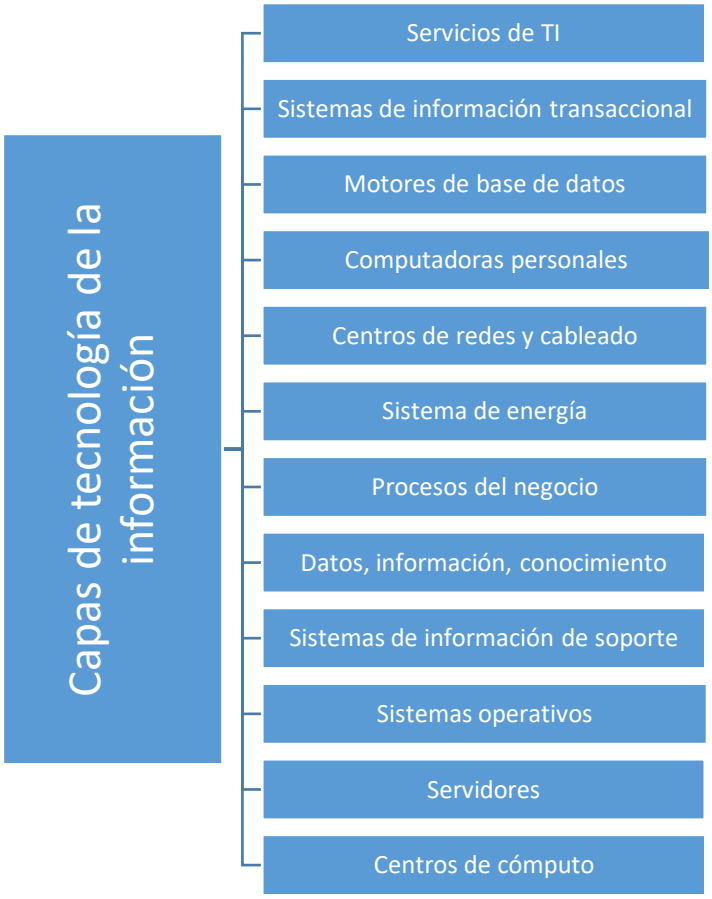


Tomado de: (Cruces & Mora, 2016)

En el artículo escrito por el autor Valencia (2015) indica que los riesgos de TI cubren la información, los activos tecnológicos y los servicios TIC, de esa consideración y de los modelos que analiza el autor, plantea un sólo modelo compuesto por capas tecnológicamente interdependientes lo que lleva a una gestión de riesgos integral (Valencia, 2015):

Figura 33.

Capas de Tecnologías de Información y Comunicaciones. Ejemplo 3



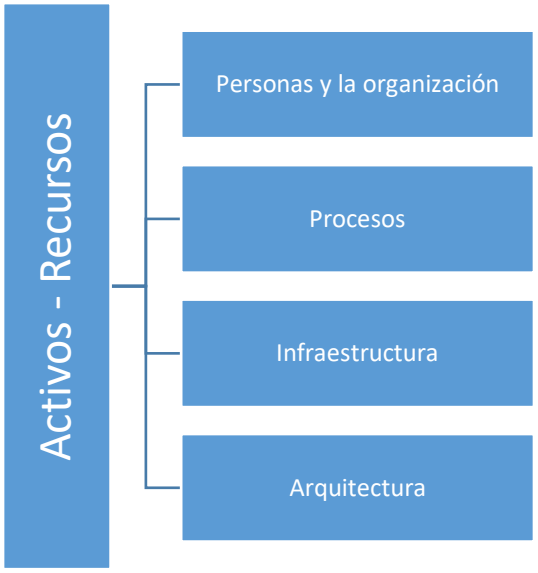
Tomado de: (Valencia, 2015)

Según las pautas de RISK IT, un activo es un componente de un escenario de riesgos.

> Un activo es cualquier objeto de valor de la organización que puede ser afectado por un evento y crear un impacto en el negocio. Un recurso es cualquier cosa que ayude a lograr los objetivos de TI. Los bienes, los activos y los recursos pueden ser idénticos, por ejemplo: los bienes informáticos son un recurso importante porque todas las aplicaciones de TI los utilizan y también son un activo porque brindan un valor a la organización. (ISACA, 2020, pág. 26).

Figura 34.

Activos o Recursos según RISK IT



Tomado de: (ISACA, 2020)

Sucesivamente, se podrían mostrar algunas otras clasificaciones de activos, lo significativo es tener la certidumbre de que un activo necesita ser gobernado y gestionado y esto aplica sobre la información, los servicios, la infraestructura, las aplicaciones, los colaboradores, sus habilidades y competencias, etc (ISACA, 2020). Por tal razón COBIT 5 (ISACA, 2012) considera a los activos como catalizadores. En términos generales, un catalizador está definido como la situación u objeto que atrae fuerzas en pos de cumplir metas.

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

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

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

Tabla 25.

Clasificación de Activos

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

Recuperado de: (ISACA, 2020)

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 5. Analizar los Riesgos:

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

a) Verificar los Escenarios de Riesgos:

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

Los escenarios de riesgos contienen elementos que se vinculan con el riesgo real de la actividad de la organización. Para RISK IT estos escenarios permiten tener una visión global de los riesgos proporcionando una estructura donde se destacan los eventos de pérdida, los efectos negativos o los daños y se diferencian de las amenazas y vulnerabilidades porque la amenaza es un problema potencial a la seguridad de un activo y la vulnerabilidad es una debilidad que puede hacer que una amenaza particular se vuelva realidad. A continuación, en la tabla 26, se muestran los ámbitos o categorías de los escenarios de riesgo y además los escenarios de riesgos que los conforman y que propone la herramienta RISK IT (ISACA, 2020):

Tabla 26.

Ámbitos o Categorías y Escenarios de Riesgos de RISK IT

	ÁMBITO DEL ESCENARIO DE RIESGO		ESCENARIO DE RIESGO
A	INFRAESTRUCTURA DE TI	01	Obsolescencia de la infraestructura de TI
		02	Daño o destrucción de la infraestructura de TI
		03	Robo a infraestructura de TI
		04	Arquitectura de infraestructura de TI inadecuada
		05	Instalación y aplicación de cambios en infraestructura de TI
B	RELACIONADOS AL PERSONAL DE TI	06	Ausencia de personal clave de TI
		07	Falta de habilidades y experiencia del personal de TI
		08	Insuficiencia de personal clave de TI
C	GESTIÓN DE PROYECTOS DE TI	09	Proyectos no finalizados
		10	Riesgo económico de proyectos
		11	Retraso en la entrega de proyectos
		12	Baja calidad en los proyectos
		13	Falta de visión del portafolio de proyectos
D	GESTIÓN DE SEGURIDAD DE TI	14	Ataques lógicos a la seguridad
		15	Transgresión de seguridad
		16	Alteración de la integridad de la información
		17	Exposición de la información
E	APLICACIONES DE TI	18	Decisiones incorrectas de inversión en aplicaciones de TI
		19	Caducidad de las aplicaciones
		20	Implementación inadecuada de aplicaciones
		21	Inestabilidad de las aplicaciones
		22	Falta de capacidad de las aplicaciones
		23	Caducidad de aplicaciones de infraestructura
		24	Aplicaciones intrusas
F	ENTREGA Y SOPORTE EN LOS SERVICIOS QUE PROVEE TI	25	Entrega y soporte de servicios de TI
		26	Rendimiento de servicios
G	CUMPLIMIENTO CORPORATIVO DE TI	27	Cumplimiento de acuerdos y compromisos
		28	Cumplimiento de licenciamiento
H	CUMPLIMIENTO LEGAL DE TI	29	Cumplimiento legal de TI (en el país)
I	OTROS ESCENARIOS DE RIESGOS DE TI	30	Rendición de cuentas de TI
		31	Integración de TI y procesos de la organización
		32	Procesos operativos de TI y de manejo de errores

Recuperado de: (ISACA, 2020)

b) Realizar Mapas de Riesgos:

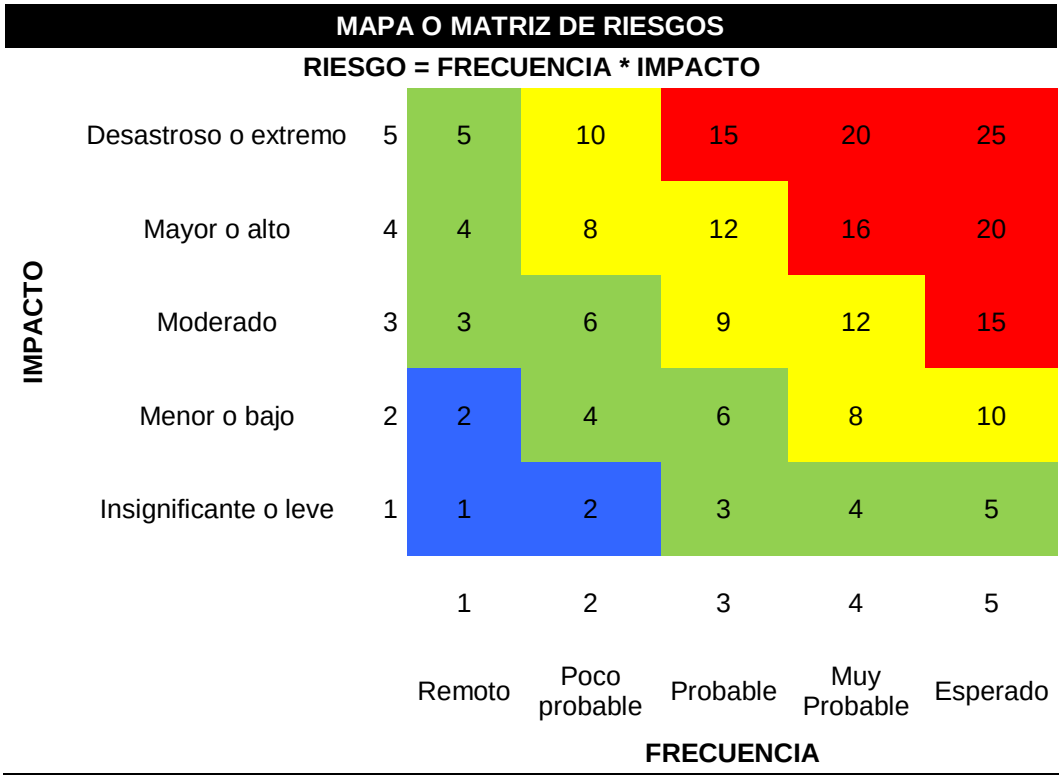
Con los escenarios definidos, lo que RISK IT recomienda a continuación, es realizar una evaluación probabilística de que ocurra un riesgo (la frecuencia) y además la consecuencia del mismo (el impacto) para verificar si estos parámetros se encuentran dentro de lo aceptable; considerando que la organización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

Estos conceptos son coherentes con los fundamentos de RISK IT, cuando se determinó el apetito frente al riesgo; se lo realizó mediante la combinación entre impacto o magnitud y la frecuencia de ocurrencia de un riesgo, el producto de esta valoración resultó en la determinación del riesgo plasmado en un mapa de riesgos (ISACA, 2020). Así mismo, se definió en el segundo capítulo del presente trabajo de titulación cuando se mostró que la forma de medir el nivel de riesgo es una estimación de lo que puede ocurrir y se valora de forma cuantitativa (o cuantificada), como la consecuencia del impacto asociado a un escenario por la probabilidad de ocurrencia del mismo.

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

Tabla 27.

Mapa o Matriz de Riesgos



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

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

Tabla 28.

Riesgo Calificado según Niveles de Bandas de Colores

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

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 6. Mantener un Perfil de Riesgos:

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

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 7. Responder al Riesgo:

En su investigación el autor Crespo (2016) indica una serie de instancias para responder al riesgo, es decir brindar al riesgo un tratamiento:

Para responder al riesgo primeramente es necesario decidir si un riesgo puede tener un tratamiento específico o puede ser tratado durante el curso de procedimientos

normalizados de gestión, es decir, integrar el tratamiento en las prácticas del día a día de la organización (Crespo, 2016).

En segundo lugar, se debe tener en cuenta lo que se quiere como deseable para el tratamiento de los riesgos para evitar, mitigar, compartir, aceptar o asumir el nivel de riesgo existente, definiciones que se explicaron en el tercer capítulo del presente trabajo de titulación.

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

Seguidamente, todas las opciones de tratamiento antes citadas pueden y deben ser combinadas con otros controles o contramedidas y luego ser aplicadas según la dotación de recursos y otras consideraciones que hayan sido aprobadas.

Finalmente, una vez que los riesgos inherentes han sido tratados se deberá evaluar el riesgo residual. El riesgo residual se refiere a la probabilidad de que el riesgo ocurra después de que ha sido tratado, es decir que sea recurrente. La calificación del riesgo residual suele ser inferior al valor original o riesgo inherente, de lo contrario se considera que los controles seleccionados no fueron eficaces (Crespo, 2016). Como un riesgo residual es latente debe ser monitoreado, documentado y evaluado continuamente.

Se debe tomar en cuenta que las contramedidas o catálogos de controles pueden variar con los avances de la tecnología, se pueden ir modificando, van

desapareciendo, aparecen nuevos o evolucionan (ISACA, 2020). Los controles de RISK IT se mostrarán en el siguiente apartado al definir un portafolio de acciones.

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

Tabla 29.

Respuesta al Riesgo Acorde al Nivel de Riesgo

NIVELES DE RIESGO	RESPUESTA AL RIESGO	DESCRIPCIÓN
Inaceptable	Evitar	La organización debe estimar que este nivel de riesgo va más allá de su apetito de riesgo normal. Un riesgo que se encuentre en esta banda, en primear instancia, podría desencadenar una respuesta inmediata. Cuando un riesgo se juzga inaceptable por la administración también entra en la categoría de evasión. Evadir o evitar un riesgo significa salir de las actividades o condiciones que dan cabida a ese riesgo. Evitar se aplica cuando no existe otra respuesta adecuada o cuando no existe ninguna respuesta rentable que pueda tener éxito en la reducción de la frecuencia y magnitud o cuando el riesgo no pueda ser compartido o transferido.
Elevado	Mitigar / Compartir	La organización podría aceptarlo, pero requiere mitigación o una respuesta adecuada dentro de límites de tiempo determinados. La mitigación significa que se deben tomar acciones para reducir la frecuencia e impacto de un riesgo. Se consigue fortaleciendo de forma general la gestión de prácticas de riesgos de TI y con la introducción de medidas de control que intenten reducir la frecuencia de un suceso adverso y/o el impacto del evento en caso de que suceda. Además, el riesgo se puede compartir o transferir, significa reducir la frecuencia o impacto mediante la transferencia o distribución de una porción del riesgo. Las estrategias comunes incluyen tener un seguro para incidentes relacionados con TI, la subcontratación de parte de las actividades de TI o establecer proyectos compartidos con un proveedor a través de acuerdos de inversión compartida. Estas técnicas no alivian a la organización de un riesgo pero pueden reducir las consecuencias económicas en el caso de producirse un evento adverso.
Aceptable	Aceptar	Indica un nivel aceptable o normal de riesgo con ninguna acción requerida excepto el mantenimiento de controles actuales. Aceptar significa que cuando un riesgo en particular se produce la pérdida sea aceptada. Esto difiere de ignorar el riesgo porque aceptar supone que el riesgo es conocido, es decir, una decisión informada se ha aceptado por la dirección o administración
Oportunidad	Asumir	Indica la existencia de un riesgo donde el ahorro de costo de oportunidad se puede encontrar al disminuir el grado de control o donde las oportunidades para asumir más riesgos pueden surgir

Adaptado de: (ISACA, 2012)

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 8: Definir un Portafolio de Acciones:

Para definir un portafolio de acciones concretas se deben recomendar controles adecuados para minimizar los riesgos identificados; evitar, mitigar, aceptar o asumir el impacto de los mismos en el ámbito técnico. Esto implica la adecuación de controles o contramedidas a ser implementadas como tratamiento de los riesgos. Para el planteamiento de controles la herramienta RISK IT tiene un portafolio para cada uno de los escenarios de riesgos (ISACA, 2020):

Tabla 30.

Controles para los Riesgos en la Infraestructura de TI

A	RIESGOS EN LA INFRAESTRUCTURA DE TI
A.01	**Controles para obsolescencia de la infraestructura de TI**
A.01.a	Evaluación de las capacidades y rendimientos actuales
A.01.b	Establecer un plan de adquisición de infraestructura tecnológica a corto, mediano y largo plazo
A.01.c	Fomentar la estandarización tecnológica
A.01.d	Establecer la dirección y criterios para la planificación tecnológica
A.01.e	Realizar mantenimiento de infraestructura de forma periódica en cumplimiento de las recomendaciones establecidas por los fabricantes y proveedores
A.02	**Controles para el daño o destrucción de la infraestructura de TI**
A.02.a	Establecer medidas de seguridad para prevenir, detectar y mitigar los riesgos asociados a robo, fuego, agua, humo, actos vandálicos entre otros
A.02.b	Definir procedimientos de seguridad de acceso físico y perimetral estableciendo las áreas restringidas y permisos de acceso por rol o cargo. Deberán incluirse las actividades para gestionar los accesos, autorizarlos, registrarlos y supervisarlos
A.02.c	Administración de instalaciones físicas. Los controles deberán incluir medidas para el cumplimiento de normas, leyes, regulaciones y reglamentos acerca de la seguridad, salud y normas operativas internas
A.03	**Controles para el robo a infraestructura de TI**
A.03.a	Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
A.03.b	Controles en procedimientos de personal de gestión en el proceso de reclutamiento, haciendo énfasis en plazas críticas, puestos claves o sensibles para la organización
A.03.c	Controles para la protección de la infraestructura a nivel de hardware y software que documenten las actividades realizadas y permitan su posterior revisión. Estos deben incluir responsables del control de componentes de infraestructura sensibles y críticos para la organización, así como actividades de supervisión
A.04	**Controles para arquitectura de infraestructura de TI inadecuada**
A.04.a	Establecer directrices para la planificación tecnológica
A.04.b	Establecer un proceso bidireccional y reciproco que tome en consideración el plan estratégico de la organización, el plan estratégico de tecnología y las capacidades de TI
A.04.c	Establecer un comité de profesionales con experiencia y conocimientos, responsables de definir lineamientos y proveer conocimientos sobre cómo realizar las implementaciones garantizando resultados sostenibles

A	RIESGOS EN LA INFRAESTRUCTURA DE TI
A.05	**Controles para la instalación y aplicación de cambios en infraestructura de TI**
A.05.a	Establecer un plan de mantenimiento para la infraestructura que incluya la administración de actualizaciones y correcciones
A.05.b	Establecer un procedimiento de gestión de cambios y garantizar que los cambios o modificaciones se realizan de acuerdo a los procedimientos definidos

Recuperado de: (ISACA, 2020)

Tabla 31.

Controles para los Riesgos Relacionados al Personal de TI

B	RIESGOS RELACIONADOS AL PERSONAL DE TI
B.06	**Controles para la ausencia de personal clave de TI**
B.06.a	Crear y mantener un inventario de personal clave que describa sus habilidades y responsabilidades
B.06.b	Minimizar la dependencia de personas claves por medio de la documentación, intercambio de conocimientos y un plan de sucesión a puestos clave; estableciendo el sucesor y las brechas a cubrir para que pueda cubrirlo en periodos de tiempo considerables
B.07	**Controles para la falta de habilidades y experiencia del personal de TI**
B.07.a	Alinear el proceso de reclutamiento a los procedimientos y normas de la organización
B.07.b	Establecer un inventario de personal y sus habilidades
B.07.c	Evaluar el desempeño de los colaboradores según sus responsabilidades, objetivos definidos y logros alcanzados
B.07.d	Mantener una política de mejora continua de las habilidades y competencias de los colaboradores para apoyarles en el cumplimiento de sus funciones y objetivos organizacionales
B.07.e	Mantener actualizados los manuales o perfiles de puesto de trabajo de TI, las competencias y los requisitos necesarios para cumplir con las funciones de los diferentes roles
B.07.f	Analizar constantemente la capacidad de TI versus la demanda actual y futura para identificar las habilidades necesarias para alcanzar los objetivos y asegurar la disponibilidad en el tiempo que sea necesario
B.08	**Controles para la insuficiencia de personal clave de TI**
B.08.a	Establecer y mantener un inventario de personal y sus habilidades

B	RIESGOS RELACIONADOS AL PERSONAL DE TI
B.08.b	Mantener actualizados los manuales o perfiles de puesto de trabajo de TI, las competencias y los requisitos necesarios para cumplir con las funciones de los diferentes roles
B.08.c	Analizar constantemente la capacidad de TI versus la demanda actual y futura para identificar las habilidades necesarias para alcanzar los objetivos y asegurar la disponibilidad en el tiempo que sea necesario

Recuperado de: (ISACA, 2020).

Tabla 32.

Controles para los Riesgos en la Gestión de Proyectos de TI

C	RIESGOS EN LA GESTIÓN DE PROYECTOS DE TI
C.09	**Controles para el riesgo de proyectos no finalizados**
09.a	Establecer un marco de trabajo para la gestión de proyectos que defina los lineamientos y mejores prácticas a cumplir
09.b	Establecer un comité de proyectos que se responsabilice de priorizar los mismos para que se encuentren alineados con la estrategia de la organización
09.c	Elaborar un conjunto de mediciones que permitan evaluar el cumplimiento de objetivos de proyectos
09.d	Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad
C.10	**Controles para riesgo económico de proyectos**
10.a	Establecer procedimientos para la administración de costos ejecutados versus presupuestados para determinar desviaciones e impacto para definir si se asigna más presupuesto o se acepta el costo de oportunidad de no asignarlo
10.b	Establecer procedimientos para la definición de presupuestos de tecnología considerando costos operativos, mantenimiento, actualizaciones, inversión y prioridades definidas
10.c	Establecer métricas de control para el cumplimiento de proyectos enfocados al cumplimiento de tiempos, costos y calidad
10.d	Establecer un comité de proyectos que se responsabilice de priorizar los mismos para que se encuentren alineados con la estrategia de la organización
10.e	Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad
C.11	**Controles para riesgo de retraso en la entrega de proyectos**

C	RIESGOS EN LA GESTIÓN DE PROYECTOS DE TI
11.a	Establecer métricas de control para el cumplimiento de proyectos enfocados al cumplimiento de tiempos, costos y calidad
11.b	Establecer métricas individuales que midan el desempeño de los recursos asignados a proyectos. Estas deberán proveer información para mejorar la estimación de tiempos de entrega, comparar estadísticas con el mercado y evaluar si es necesario realizar cambios, entrenamiento, balancear cargas de trabajo, modificar procedimientos, entre otros
11.c	Establecer un comité de proyectos que se responsabilice de priorizar los mismos para que se encuentren alineados con la estrategia de la organización
11.d	Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad
C.12	**Controles para riesgos por baja calidad en los proyectos**
12.a	Establecer un marco de trabajo para la gestión de proyectos que defina los lineamientos y mejores prácticas a cumplir
12.b	Implementar procedimientos de aseguramiento de calidad cuyas actividades deben ser parte de los planes de desarrollo de proyectos
12.c	Establecer un comité de profesionales con experiencia y conocimientos, responsables de definir lineamientos y proveer conocimientos sobre cómo realizar las implementaciones garantizando resultados sostenibles
12.d	Establecer compromisos con los Stakeholders (partes interesadas) de tal forma que participen en la definición y ejecución de las actividades de proyectos, haciéndolos parte del mismo para aprovechar el conocimiento en los procesos y de la organización
12.e	Fomentar la estandarización tecnológica definiendo normas y estándares para el ciclo de vida de proyectos
12.f	Asegurar que los dueños de procesos, personal de tecnología, aseguramiento de calidad e interesados, aprueben el resultado de las pruebas de acuerdo al plan de pruebas establecido
12.g	Certificar que se obtienen los resultados esperados al finalizar los proyectos, informar a los patrocinadores, usuarios y equipo del proyecto documentando las lecciones aprendidas y definiendo planes de acción si no se cumple con los requerimientos.
C.13	**Controles para la falta de visión del portafolio de proyectos**
13.a	Establecer un marco de trabajo para la gestión de proyectos que defina los lineamientos y mejores prácticas a cumplir
13.b	Establecer métricas de control para el cumplimiento de proyectos enfocados al cumplimiento de tiempos, costos y calidad
13.c	Establecer un comité de proyectos que se responsabilice de priorizar los mismos para que se encuentren alineados con la estrategia de la organización
13.d	Establecer acuerdos de servicios con indicadores de desempeño que midan el cumplimiento y efectividad, para garantizar el ciclo de mejora continua
13.e	Establecer mediciones para monitorear y evaluar el cumplimiento de objetivos
13.f	Definir procedimientos para la elaboración de informes de revisiones periódicas al portafolio de proyectos evaluando el cumplimiento y su efectividad

Recuperado de: (ISACA, 2020)

Tabla 33.

Controles para los Riesgos en la Gestión de Seguridad de TI

D	RIESGOS EN LA GESTION DE SEGURIDAD DE TI
D.14	**Controles para ataques lógicos a la seguridad**
14.a	Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
14.b	Desarrollar y mantener un BCP (Business Continuity Plan) con instrucciones claras para recuperar los servicios críticos de TI, con responsabilidades y procedimientos de comunicación
14.c	Establecer planes de pruebas periódicas de seguridad, implementar mecanismos de vigilancia, monitoreo y control, que alerten y reporten eventos detectados de violación de seguridad
14.d	Establecer mecanismos de prevención, detección y corrección de intromisiones de software malicioso, así como procedimientos de actualizaciones de seguridad y antivirus
14.e	Establecer procedimientos y normas de seguridad de red que incluyan técnicas y procesos de asignación o denegación de accesos, control de flujos de información, entre otros
14.f	Establecer procedimientos para gestionar la seguridad de información que incluyan la descripción de actividades para recepción, almacenamiento y salida de datos
14.g	Establecer los criterios de definición de los propietarios de datos, sistemas y procesos por parte de las áreas de la organización responsables de la información
D.15	**Controles para la transgresión de seguridad**
15.a	Establecer procedimientos para la administración de usuarios, roles y accesos, definiendo procesos claros de autorización, altas, bajas y modificaciones de usuarios
15.b	Garantizar que los usuarios se identifiquen de forma única e inequívoca por medio de la autenticación para poder acceder a los recursos, servicios y aplicativos
15.c	Proveer y mantener una matriz de perfil de puestos y funciones que identifique el perfil de accesos estándar y permita autorizar y documentar excepciones
15.d	Establecer planes de pruebas periódicas de seguridad, implementar mecanismos de vigilancia, monitoreo y control, que alerten y reporten eventos detectados de transgresión de seguridad
15.e	Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
15.f	Establecer procedimientos que aseguren el conocimiento y compromiso de los usuarios al cumplimiento de las políticas enfocadas a la protección y uso de los activos de información y recursos tecnológicos de la organización
D.16	**Controles para el riesgo de alteración de la integridad de la información**
16.a	Establecer los criterios de definición de los propietarios de datos, sistemas y procesos por parte de las áreas de la organización responsables de la información

D	RIESGOS EN LA GESTION DE SEGURIDAD DE TI
16.b	Establecer un procedimiento para la gestión de cambios de aplicaciones, procesos, sistemas, configuraciones de componentes de infraestructura de hardware y software; que defina actividades de aprobación, categorización y priorización
16.c	Mantener actualizado el inventario de activos de TI que incluya su tipificación e interrelación
16.d	Definir procedimientos para la generación de respaldos y recuperación de información que permita clasificarla y especifique qué información se excluye o incluye, así como los periodos de tiempo en los cuales estarán disponibles
D.17	**Controles para la exposición de la información**
17.a	Definir la política de traslado de información sensible que especifique que los datos sensibles sólo podrán ser trasladados por medios estandarizados autorizados y aprobados
17.b	Definir una política del uso de internet, correos electrónicos personales y el uso de dispositivos externos que pueden conectarse a la red interna
17.c	Establecer un procedimiento que garantice que todos los colaboradores tienen conocimiento y se comprometen a cumplir las políticas enfocadas a la protección de los activos de información y recursos tecnológicos de la organización
17.d	Establecer mecanismos de protección de activos de información en equipos estacionarios y en especial para equipos móviles los cuales presentan una mayor exposición a riesgos

Recuperado de: (ISACA, 2020)

Tabla 34.

Controles para los Riesgos en Aplicaciones de TI

E	RIESGOS EN APLICACIONES DE TI
E.18	**Controles para decisiones incorrectas de inversión en aplicaciones de TI**
18.a	Establecer un comité de proyectos que se responsabilice de priorizar los mismos para que se encuentren alineados con la estrategia de la organización
18.b	Establecer compromisos con los Stakeholders (partes interesadas) de tal forma que participen en la definición y ejecución de las actividades de proyecto, haciéndolos parte del mismo para aprovechar el conocimiento en los procesos y de la organización
18.c	Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión de proyectos
18.d	Establecer métricas de control para el cumplimiento de proyectos enfocados al cumplimiento de tiempos, costos y calidad

E	RIESGOS EN APLICACIONES DE TI
18.e	Analizar constantemente la capacidad de TI versus la demanda actual y futura para identificar las habilidades necesarias para alcanzar los objetivos de la organización y asegurar la disponibilidad en el tiempo que sea necesario
E.19	**Controles para la caducidad de las aplicaciones**
19.a	Fomentar la estandarización tecnológica
19.b	Establecer la dirección para la planificación tecnológica
19.c	Establecer procedimientos para dar mantenimiento a las aplicaciones de software que incluyan evaluaciones periódicas para implementar mejoras en diseño y funcionalidad
19.d	Evaluar la capacidad actual y el rendimiento de las soluciones entregadas y compararlas con las necesidades futuras
E.20	**Controles para la implementación inadecuada de aplicaciones**
20.a	Implementar dentro de los procedimientos de desarrollo las fases de planificación, la especificación y puntos de control para alcanzar la calidad en los proyectos
20.b	Planificar y ejecutar la transferencia de conocimiento para el personal operativo y de soporte
20.c	Establecer un plan de implementación y de contingencia de proyectos aprobados por los interesados
20.d	Asegurar que los responsables de procesos, personal de tecnología, aseguramiento de calidad e interesados, aprueben el resultado de las pruebas de acuerdo al plan de pruebas establecido
E.21	**Controles para el riesgo de inestabilidad de las aplicaciones**
21.a	Establecer procedimientos para dar mantenimiento a las aplicaciones de software
21.b	Monitorear periódicamente el rendimiento y la capacidad de las aplicaciones y recursos de TI para asegurar que cumplan con los niveles de servicio acordados con los usuarios y obtener el estado real de las aplicaciones
21.c	Garantizar que los responsables de procesos, personal de tecnología, personal de aseguramiento de calidad aprueben el resultado de las pruebas de acuerdo al plan de pruebas establecido
21.d	Establecer un procedimiento para la administración de problemas que permita la trazabilidad de problemas, e incluya información referente al problema como: detalle de errores, causas raíz, recursos afectados, recursos utilizados, tiempos de los eventos y solución aplicada
E.22	**Controles para el riesgo de falta de capacidad de las aplicaciones**
22.a	Monitorear periódicamente el rendimiento y la capacidad de las aplicaciones y recursos de TI para asegurar que cumplan con los niveles de servicio acordados con los usuarios y obtener el estado real de las aplicaciones
22.b	Realizar mantenimiento de infraestructura donde están instaladas las aplicaciones de forma periódica en cumplimiento de las recomendaciones establecidas por los fabricantes y proveedores

E	RIESGOS EN APLICACIONES DE TI
E.23	**Controles para el riesgo de caducidad de aplicaciones de infraestructura**
23.a	Establecer la dirección y criterios para la planificación tecnológica
23.b	Establecer un plan de adquisición de infraestructura tecnológica a corto, mediano y largo plazo
23.c	Realizar mantenimiento de infraestructura de forma periódica en cumplimiento de las recomendaciones establecidas por los fabricantes y proveedores
E.24	**Control para el riesgo de aplicaciones intrusas**
24.a	Establecer mecanismos de prevención, detección y corrección de intromisiones de software malicioso, así como procedimientos de actualizaciones de seguridad y antivirus

Recuperado de: (ISACA, 2020)

Tabla 35.

Controles para los Riesgos en los Servicios que Provee TI

F	RIESGO EN LOS SERVICIOS QUE PROVEE TI
F.25	**Controles para el riesgo en la entrega y soporte de servicios de TI**
25.a	Establecer un procedimiento para la selección de proveedores que sea transparente e imparcial, asimismo que incluya la creación, modificación y cancelación de contratos con proveedores
25.b	Establecer una normativa que dicte los lineamientos para establecer acuerdos de servicio con los proveedores y los compromisos que sean adquiridos por ambas partes
25.c	Establecer contratos con proveedores apegados a las normativas internas y legales; clarificar los términos de seguridad, sanciones o penalizaciones y reconocimientos
25.d	Establecer un proceso que permita definir y reunir las métricas que midan el cumplimiento de los acuerdos de servicios, incluyendo acuerdos de servicio provistos por los proveedores
F.26	**Controles para riesgos de rendimiento de servicios**

F	RIESGO EN LOS SERVICIOS QUE PROVEE TI
26.a	Definir los acuerdos de niveles de servicio como mínimo para los que son críticos, basándose en la capacidad de TI y los requisitos de los interesados con quienes deberán acordarse considerando la disponibilidad, fiabilidad, restricciones, seguridad, rendimiento, continuidad y tiempos de respuesta
26.b	Diseñar un plan de recuperación y reanudación de servicios de TI
26.c	Establecer un proceso que permita definir y reunir las métricas que midan el cumplimiento de los acuerdos de servicios, incluyendo acuerdos de servicio provistos por los proveedores
26.d	Desarrollar y mantener un BCP (Business Continuity Plan) con instrucciones claras para recuperar los servicios críticos de TI, con responsabilidades y procedimientos de comunicación

Recuperado de: (ISACA, 2020)

Tabla 36.

Controles para los Riesgos en el Cumplimiento Corporativo de TI

G	RIESGOS EN EL CUMPLIMIENTO CORPORATIVO DE TI
G.27	**Control para riesgos en el cumplimiento de acuerdos y compromisos**
27.a	Establecer una normativa que dicte los lineamientos para establecer acuerdos de servicio con los proveedores y los compromisos que sean adquiridos por ambas partes
G.28	**Controles para riesgos en el cumplimiento de licenciamiento**
28.a	Identificar las regulaciones locales e internacionales referentes a la propiedad intelectual y derechos sobre licenciamiento
28.b	Establecer políticas para prohibir el uso de software sin licenciamiento y que regule el uso de software libre en la organización

Recuperado de: (ISACA, 2020)

Tabla 37.

Controles para los Riesgos en el Cumplimiento Legal de TI

H	RIESGOS EN EL CUMPLIMIENTO LEGAL DE TI
H.29	**Controles riesgos en el cumplimiento legal de TI**
29.a	Identificar las regulaciones locales e internacionales referentes a normas de la industria y laborales que se encuentren relacionadas a las políticas y procedimientos internos de TI
29.b	Establecer derechos de propiedad intelectual internos para el desarrollo de software y programas informáticos por parte del personal de tecnología como parte de sus funciones. Estos deberán quedar estipulados por medio de documentos definidos por la organización y aceptados por el personal de tecnología

Recuperado de: (ISACA, 2020)

Tabla 38.

Controles para Otros Escenarios de Riesgos de TI

I	OTROS ESCENARIOS DE RIESGOS DE TI
I.30	**Control de riesgos en la rendición de cuentas de TI**
30.a	Establecer políticas internas de TI que regulen el comportamiento, describan los roles, responsabilidades y rutas para la rendición de cuentas de los diferentes roles responsables de la gestión
I.31	**Controles de riesgos de integración de TI y procesos de la organización**
31.a	Establecer un proceso que fomente la educación y comunicación bidireccional de la planeación estratégica de TI con la organización
31.b	Establecer un procedimiento y mecanismos que faciliten la coordinación, comunicación e interacción entre el personal de TI y las partes interesadas
I.32	**Controles de riesgos en procesos operativos de TI y de manejo de errores**
32.a	Establecer un procedimiento de entrenamiento y capacitación para personal de nuevo ingreso que contemple la formación continua alineada a las funciones de los roles para alcanzar los objetivos organizacionales
32.b	Definir y documentar los procedimientos operacionales de TI

32.c Diseñar un plan de recuperación y reanudación de servicios de TI

Recuperado de: (ISACA, 2020)

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

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

Refiérase al Anexo Único para encontrar el documento para el caso específico de la Dirección de Informática de la PUCE.

Paso 9: Consultar, Comunicar y Expresar:

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

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

- Contribuye a la gestión ejecutiva para la comprensión de la exposición a los riesgos.
- Establece un comportamiento hacia las políticas que se tomen en el ámbito de los riesgos.

- Provee de transparencia a las partes interesadas en la toma de decisiones sobre riesgos.
- Establece un comportamiento hacia los resultados negativos, es decir, acontecimientos de pérdidas u oportunidades perdidas con el fin de adaptarse y tomarlos como situaciones aprendidas (ISACA, 2020).

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

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

Conclusiones y Recomendaciones

Conclusiones

Producto del presente trabajo de titulación se han podido realizar las siguientes conclusiones:

- Antiguamente, se tenía una noción del riesgo relacionado con informática después de verificar que los resultados no eran los esperados o los planificados. Es decir, después de la comprobación de una la falla sobre algún elemento de hardware o software. Posteriormente, en las organizaciones se tomó conciencia de que debía buscarse el origen de los riesgos y se documentó la magnitud de los mismos clasificándolos de diferentes maneras. En la actualidad, cuando se planifica sobre los riesgos se consideran varios factores como la medición del impacto y la frecuencia de ocurrencia de los mismos, los costos asociados, el recurso humano relacionado con la gestión de riesgos, los controles o contramedidas. Estos factores constituyen la base para la llamada gestión de riesgos. Con lo expuesto anteriormente, se puede concluir que se ha pasado de un conocimiento limitado a un conocimiento acumulado para administrar los riesgos de manera apropiada y además se tiende hacia procesos de mejora en la gestión de riesgos.
- Una vez recabada la literatura disponible se puede deducir que un riesgo es el efecto de la incertidumbre; la combinación de la probabilidad de un evento riesgoso y su ocurrencia e implica pérdida o afectación. Entonces, la gestión de riesgos se desarrolló con el propósito de proteger los activos y la información en pos de conseguir los objetivos y metas de la organización o empresa; a través de la identificación de eventos potenciales de riesgo y la inclusión de actividades coordinadas para dirigir, controlar y proteger a la organización con respecto al riesgo. Por lo tanto, se puede concluir que la gestión de riesgos establece

estrategias para que las empresas sean capaces de absorber perturbaciones sin alterar significativamente su estructura y funcionalidad.

- Luego de haber culminado con la revisión de varios marcos, modelos y metodologías de gestión de riesgos desarrolladas y vigentes actualmente, se puede concluir que existen etapas o fases que describen una metodología integral; iniciando con el establecimiento del contexto, la identificación de los riesgos, la evaluación y valoración de los mismos y el plan específico de tratamiento. Con lo cual, se puede colegir que todas aquellas fases citadas, finalmente conducen a la evasión, reducción, compartición o retención de los riesgos, todas estas opciones de tratamiento deben ser evaluadas por su alcance, su costo y los beneficios derivados para la organización.
- La herramienta RISK IT abarca una metodología para gestión de riesgos en base a ámbitos y procesos, los ámbitos son clasificaciones amplias y contienen a los procesos. De la misma forma, para la metodología propuesta en el presente trabajo de titulación; *gobernar el riesgo, administrar el riesgo y definir el apetito y tolerancia ante el riesgo* son procesos propios de *gobernar el riesgo*. *Recopilar datos, analizar los riesgos y mantener un perfil de riesgos* son fases de la *evaluación del riesgo*. *Responder al riesgo, definir un portafolio de acciones y comunicar y expresar* son etapas de la *respuesta ante el riesgo*. Por lo tanto, se puede concluir que los ámbitos y procesos propuestos son congruentes con la metodología de RISK IT cuyos ámbitos son *gobernar el riesgo, evaluar el riesgo y respuesta ante el riesgo.*
- Para el presente trabajo de titulación fue necesario el desarrollo de una ruta general de investigación previo al abordaje de la metodología técnica basada en RISK IT. Por tal motivo, se determinó que la investigación se enmarcaría en la ruta de investigación mixta cuya meta no es reemplazar a la investigación cuantitativa

ni a la investigación cualitativa, sino utilizar las fortalezas de ambos tipos de indagación, combinándolas. Se documentaron las ventajas de este tipo de ruta de investigación que señala que se debe determinar un diseño de la investigación, una unidad de análisis, así como realizar una recolección de datos y un análisis de los mismos, por último, es propicio generar resultados e inferencias y realizar un reporte. Entonces se puede concluir que antes de realizar el trabajo técnico es necesario definir una ruta general de investigación que sea una guía para la misma.

- Algunos de los componentes que pertenecen a Gobernar el riesgo son las nociones de apetito ante el riesgo y tolerancia por el riesgo que son conceptos diferentes. El apetito por el riesgo está relacionado con la cantidad o magnitud de riesgo que la organización está dispuesta a aceptar para alcanzar una meta, mientras que la tolerancia al riesgo es la variación desde el nivel establecido por el apetito para conseguir la misma meta después de haber sucedido un evento riesgoso. Con lo expuesto, se puede concluir que son conceptos distintos, pero están relacionados complementariamente y dependen de las políticas que los directivos de las organizaciones hayan establecido y por lo tanto existirán tantos niveles de apetito y tolerancia al riesgo como organizaciones que decidan adoptar estos conceptos en su cultura de riesgos y llevarlos a la práctica.
- Una vez que se han determinado los activos de la organización, a los mismos, se les debe ubicar en categorías y escenarios de riesgos como lo determina la herramienta RISK IT con el propósito de realizar el análisis de riesgos sobre esos activos. Con lo cual se puede concluir que, a diferencia de otras metodologías orientadas a riesgos, RISK IT se concentra en las categorías de riesgo y los escenarios de los mismos más no en determinar amenazas ni vulnerabilidades. La diferencia es que la amenaza es un problema potencial a la seguridad de un activo

y la vulnerabilidad es una debilidad que puede hacer que una amenaza particular se vuelva realidad; por el contrario, para RISK IT manejar el análisis de riesgos mediante categorías y escenarios le permite tener una visión global e integral de los riesgos proporcionando una estructura donde se destacan los eventos de pérdida, los efectos negativos o los daños sobre los activos.

- Al determinar los activos, las categorías de riesgos y los escenarios de riesgos a los que están expuestos los activos, se debe realizar una valoración de riesgos sobre los mismos, dando como resultado un número que se obtiene del cálculo de la probabilidad (frecuencia) de ocurrencia de un riesgo por el impacto que ese riesgo causa sobre un activo; este proceso es necesario para que el valor pueda ser plasmado en un mapa de riesgos debido a que un mapa de riesgos es un instrumento con utilidad en la identificación de una acción de gestión de riesgos requerida. Con lo anteriormente descrito, se puede inferir que para el área de Redes e Infraestructura de la Dirección de Informática la mayor valoración de riesgo está sobre los escenarios *obsolescencia, daño o destrucción y robo de la infraestructura de TI* que influyen sobre el activo *Banner aplicación, Banner Oracle y Sap aplicación* que pertenecen a los *servidores de producción* del área. Así mismo, para los riesgos relacionados con el Recurso Humano la mayor valoración recae sobre los escenarios de riesgo *procesos operativos de TI y de manejo de errores* que influyen sobre el activo *Secretaria Ejecutiva.* Además, para los Riesgos Relacionados a Recurso Humano la mayor valoración de riesgo está sobre el escenario *falta de habilidades y experiencia del personal clave de TI* que influyen sobre el activo *Jefe de Base de Datos.* En el mapa de riesgos se calificaron como *riesgos inaceptables*. Cabe anotar que se registra un activo llamado *Auxiliar Administrativo* del área de Operaciones que alcanza un nivel de *Oportunidad.*

- Posteriormente a determinar los activos de la organización, las categorías, los escenarios de riesgos, realizar la valoración de los riesgos y plasmar los mapas de riesgos; RISK IT sugiere mantener un perfil de riesgos conocidos actualizado. El perfil de riesgos es la última etapa de la evaluación del riesgo y por lo tanto se puede concluir que permite prepararse a la siguiente fase que es la respuesta ante el riesgo.
- Concluidas las etapas de gobernar el riesgo y evaluación del riesgo se debe responder al riesgo. Responder al riesgo implica brindar un tratamiento en torno a evitar, mitigar o compartir, aceptar y asumir los riesgos. Las opciones de tratamiento antes citadas pueden y deben ser combinadas con otros controles o contramedidas. Después de realizado el estudio se puede concluir que en las áreas de Desarrollo de Software, Operaciones y Base de Datos como los activos se ubicaron en niveles de riesgo *aceptable y elevado* el tratamiento adecuado es *aceptar y mitigar/compartir* respectivamente. Pero en el área de Redes e Infraestructura los riesgos se situaron en niveles *aceptable, elevado e inaceptable* con lo cual, a más de *aceptar y mitigar/compartir* se debe *evitar.* Sobre los riesgos relacionados con el Recurso Humano el personal de la Dirección de Informática al ser considerado un activo se ubicó en todos los niveles y por lo tanto se concluye que se le debe dar un tratamiento o respuesta al riesgo en el orden de *evitar, mitigar/compartir, aceptar y asumir*.
- Con las opciones de tratamiento evitar, mitigar o compartir, aceptar y asumir los riesgos se deben combinar controles o contramedidas, RISK IT tiene un portafolio de ciento diez y seis controles para cada uno de los escenarios de riesgos. Una vez que los mismos se han implementado, se puede realizar un monitoreo a través del cálculo del riesgo residual que es posterior a la implementación de los controles de manera que se responda a procesos de mejora continua. Con lo

anteriormente referido, se concluye que si la valoración del riesgo residual continúa siendo similar a la valoración del riesgo inherente (antes de cualquier contramedida), los controles aplicados no han sido eficientes.

Recomendaciones

Para finalizar el presente trabajo de titulación se anotan las siguientes recomendaciones:

- Debido a la importancia que poseen las tecnologías de la información para apoyar en la consecución de las metas de las organizaciones y además proporcionar beneficios en competitividad, los riesgos que también implica adoptarlas deberían ser tratados como los demás riesgos claves; tal como los riesgos de mercado, de crédito u operativos. Entonces, la mayoría de decisiones de una organización o empresa requieren que la alta dirección o los gerentes sopesen los riesgos y los beneficios y estas decisiones no sean relegadas a especialistas técnicos debido a que los riesgos de TI no son puramente una cuestión técnica. Indudablemente, se necesitan expertos en la materia para entender y gestionar los aspectos de riesgos de TI pero el conocimiento sobre la gestión del negocio es lo más importante y por consiguiente los directivos son corresponsables por la gestión de riesgos. Un marco de riesgos como RISK IT permite a las partes interesadas (directivos, gerentes y técnicos) adoptar decisiones apropiadas con conocimiento acerca de la magnitud de los riesgos para deducir cómo responder a los mismos. Por tales motivos, desde el punto de vista metodológico se recomienda aplicar esta metodología empleada en el presente estudio en investigaciones de otras instituciones o en otras áreas de la Pontificia Universidad Católica del Ecuador.
- Al revisar la información sobre el documento FODA de la Dirección de Informática de la Pontificia Universidad Católica del Ecuador se pudieron avizorar, como debilidades, que existen políticas y procedimientos no actualizados, un análisis de riesgos insuficiente y una carencia de documentos sobre políticas de gobierno de TI aprobados por el Consejo Superior de la institución educativa. Son debilidades

que la Dirección de Informática puede compensar debido a que también se observaron ciertas fortalezas como la gestión responsable y autoridades comprometidas, un talento humano calificado y comprometido con el cambio y la capacidad de adaptación y aprendizaje de todos los miembros de la dirección. En tal sentido, se recomienda que según la dotación de recursos y otras consideraciones que hayan sido aprobadas se tomen acciones necesarias para hacer que temas como los abordados en el presente trabajo de titulación lleguen a la instancia de implementación.

- Los proyectos que actualmente se encuentra desarrollando la Dirección de Informática y los que tiene planificado desarrollar, son importantes para la institución educativa porque le dan relevancia a la Dirección de Informática, le permiten ejercitar su vocación de servicio y beneficiar a los usuarios (docentes, estudiantes y personal administrativo) con el desarrollo de soluciones, puesta en marcha de infraestructura y equipamiento y la resolución de incidentes o eventos. Por tales razones, se recomienda continuar con todos aquellos proyectos como lo son Mesa de Ayuda y Gobernanza de TI.
- Después de aplicar toda metodología de gestión de riesgos se realiza una etapa de comunicación de riesgos, que implica entender los mismos, expresarlos y discutirlos. Para lo cual, se recomienda que la organización, en este caso la Dirección de Informática, establezca un plan que implique relacionar a las fuentes y destinatarios de la información sobre riesgos, las formas y canales en que se comunicarán los mismos y la periodicidad con que se realizará este proceso y que todos estos factores, con el tiempo, formen parte de una cultura de riesgos concreta y propia de la organización.
- El presente trabajo de titulación está orientado al ámbito educativo pero cualquier institución, empresa u organización podría ajustar a sus necesidades una

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

Referencias

AEC. (2021). AEC. Obtenido de COSO: https://www.aec.es/web/guest/centro-conocimiento/coso#:~:text=COSO%20(Committee%20of%20Sponsoring%20Organizations,el%20control%20interno%2C%20y%20la

Alfaro, J. C. (Junio de 2017). Metodología para la Gestión de Riesgos de TI basada en COBIT 5. Cartago, Costa Rica.

Álvarez Romero, C. (Octubre de 2016). Análisis de Riesgos Informáticos de la Dependencia División de Sistemas Adscrita a la Subdivisión Académica de la UFPSO. Ocaña, Colombia: UFPS.

Ávalos, V. (Julio de 2007). Desarrollo de una Aplicación para Gestión de Riesgos en los Sistemas de Información Utilizando la Guía Metodológica NIST. Quito, Pichincha, Ecuador.

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática.* México: Grupo Editorial Patria.

Carrillo, J. (Agosto de 2012). Guía y Anlaisis de Gestión de Riesgos en la Adquisición e Implantación de Equipamiento y Servicios de TIC para Proyectos de Alcance Nacional. Quito, Pichincha, Ecuador.

CEDIA. (2018). *RRAAE*. Obtenido de http://www.rraae.cedia.edu.ec

Chambi, R. (2018). Modelo de Gestión de Riesgos de TI bajo COBIT 5. La Paz, Bolivia.

Cienfuegos, I. (2013). *Risk Management Theory.*

Citicus. (Julio de 2020). *Citicus*. Obtenido de http://www.citicus.com

Crespo, P. (Noviembre de 2016). Metodología de Seguridad de la Información para la Gestión del Riesgo Informático Aplicable a MPYMES. Cuenca, Azuay, Ecuador.

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

Dirección de Informática. (Todos los derechos reservados 2018). *Servicios Tecnológicos*. Obtenido de Dirección de Informática: https://www.puce.edu.ec/sitios/di/

Doria, A. (marzo de 2014). *Riesgo y Control Informático*. Obtenido de http://itriesgosycontrol.blogspot.com/

EALDE. (2020). *EALDE Bisiness School*. Obtenido de http://ealde.es

Equipo de la Dirección de Informática. (Todos los derechos reservados 2020). Plan Estratégico, Dirección de Informática de la PUCE. Quito, Pichincha, Ecuador.

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

Estupiñán Gaitán, R. (2006). *Administración del Riesgos ERM y la Auditoría Interna.* Bogotá: Ecoe Ediciones.

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

Hernández, R., & Mendoza, C. (2018). *Metodología de la Investigación.* Ciudad de México: McGraw Hill.

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

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

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

ISACA. (2019). Procesos Catalizadores. EEUU.

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

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

ISACA. (2020). *RISK IT Marco de Riesgos de TI.*

ISO. (2014). Guía ISO/CEI. *Gestión de Riesgos*.

ISO. (2016). Comité de Redacción de Gestión de Riesgos. *ISO 31000*.

ISO. (septiembre de 2018). *Online Browsing Platform*. Obtenido de OBP: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en:term:3.1

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

ISO Tools. (2020). Norma ISO 31000. El Valor de la Gestión de Riesgos en las Organizaciónes.

ISO/IEC. (2011). *International Organization for Standarization*. Obtenido de https://www.iso.org/home.html

ISO/IEC 27001. (2013). *International Organization for Standardization.* Obtenido de ISO: https://www.iso.org/search.html?q=27001

Jaramillo Andrade, J. (2013). Propuesta de Gestión del Riesgo de Infraestructura Tecnológica Basada en COBIT, para la Empresa Soft Warehouse S.A. Quito, Pichincha.

Jaramillo, J. (2013). Propuesta de Gestión de Riesgo de Infraestructura Tecnológica basada en COBIT, para la Empresa Soft Warehouse S.A. Quito, Pichincha, Ecuador.

Martín Romeral, L., & Torres Gallego, Á. (2016). Gestión de los Riesgos Tecnológicos. *SILO.TIPS*, 14-22.

Maya, P. (Junio de 2016). Plan de Implementación de SGSI. Cataluña.

Minchala, P. (2016). Estudio Comparativo de las Metodologías COBIT y COSO III para la Gestión de Riesgo de TI. Cuenca, Azuay, Ecuador.

MINTEL. (2019). Obtenido de Ministerio de Telecomunicaciones y de la Sociedad de la Información: Ministerio de Telecomunicaciones y de la Sociedad de la Información

National Institute of Standards and Technology, NIST. (2021). *NIST*. Obtenido de https://www.nist.gov/

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

OEA. (2019). Ciberseguridad Marco NIST.

Organización de Estados Iberoamericanos Para la Educación la Ciencia y la Cultura. (2019). Obtenido de https://www.oei.es/

País, E. (2019). *El potencial tecnológico de América Latina*. Obtenido de https://elpais.com/elpais/portada_america.html

Planta Física PUCE. (2019). Plano de Implantación General. Quito, Pichincha, Ecuador.

PMBOK. (2016). PMBOK. Guide and Standards. EEUU.

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

Ramirez, A., & Ortiz, Z. (2011). Gestión de Riesgos Tecnológicos basada en ISO 31000 e ISO 27005 y su Aporte a la Continuidad de Negocios. *Ingeniería*, 56-66.

Real Academia Española. (Septiembre de 2020). *Diccionario de la Lengua Española*. Obtenido de https://dle.rae.es/riesgo

Standards Australia. (2004). AS/NZS 4360:2004. Nueva Zelanda.

UNESCO. (2012). *Centro Nacional de Estudios para el Desarrollo de la Sociedad de la Infomación.* Obtenido de http://www.cetic.br

Valencia, F. J. (2015). Gobierno y Gestión de Riesgos de TI y Aspectos Diferenciadores con el Riesgo Organizacional. *Gerencia Tecnológica Informátcia*, 65-77.

Vanegas, G., & Pardo, C. (2014). *Red de Revistas Científicas de América Latina, el Caribe, España y Portugal.* Obtenido de Sistema de Información Científica: www.redalyc.org

welivesecurity. (2020). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/

Westerman, G. (Diciembre de 2006). *Sloan School of Management.* Obtenido de Center for Information Systems Research: https://dspace.mit.edu/bitstream/handle/1721.1/39809/4658-07.pdf

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