UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"MARCO DE TRABAJO RISK IT EN LA GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN LA CAJA RURAL DE AHORRO Y CRÉDITO LOS ANDES S.A. - 2015"

TESIS

PRESENTADO POR:

JHON YEFFER VENEGAS CARAZAS

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO - PERÚ

2017

Universidad Nacional del Altiplano

FACULTAD DE INGENIERIA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"MARCO DE TRABAJO RISK IT EN LA GESTIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN LA CAJA RURAL DE AHORRO Y CRÉDITO LOS ANDES S.A. - 2015"

TESIS PRESENTADA POR:

JHON YEFFER VENEGAS CARAZAS

PARA OPTAR EL TÍTULO PROFESIONAL DE: INGENIERO DE SISTEMAS

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE :.....
Mg. ELMER COYLA IDME

PRIMER MIEMBRO :.....
MSc. MILDER ZANABRIA ORTEGA

SEGUNDO MIEMBRO :.....
Dr. ELVIS AUGUSTO ALIAGA PAYEHUANCA

DIRECTOR DE TESIS :.....
Dr. HENRY IVAN CONDORI ALEJO

PUNO - PERU

2017

ÁREA: OPTIMIZACIÓN
TEMA: GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

AGRADECIMIENTO

Este proyecto de tesis me ha permitido aprovechar la competencia y la experiencia de muchas personas que deseo agradecer en este apartado.

A mis jurados y director de tesis mis más sinceros agradecimientos por su apoyo brindado durante la toda elaboración de este proyecto de investigación.

Al Lic. Javier Mendoza Nina, Ex Gerente de Riesgos; un especial agradecimiento a él porque marcó mi presente y futuro profesional con sus conocimientos y experiencia, y además porque de él aprendí que la sencillez como persona es lo más importante.

A todos mis docentes, no sólo de la Escuela Profesional de Ingeniería de Sistemas sino de toda la vida, por compartir sus conocimientos durante todos mis años de estudio.

A mis padres y a mis hermanitos por su incondicional apoyo, ya que sin ellos nada hubiera sido posible.

A todas las personas que conocí, por su amistad, apoyo, ánimo y compañía en las diferentes etapas de mi vida.

A todos ellos(as), sin importar en donde estén o si alguna vez llegan a leer estas palabras quiero darles las gracias, siempre tendrán mi mayor reconocimiento y gratitud.

DEDICATORIA

A Dios, por haber estado conmigo en cada paso que doy, por haber cuidado de mí, por haberme dado fortaleza y salud para lograr mis objetivos y sobre todo por haberme dado una familia maravillosa.

A mi mami Lucia, por su incondicional apoyo, por su amor, cariño y comprensión, por sus consejos, por haberme dado todo lo que soy como persona, mis valores, mis principios, mi carácter y mi perseverancia, por creer en mí y porque todo lo que soy se lo debo a ella. Mami, no me equivoco si digo que eres la mejor mamá del mundo, gracias por todo.

A mi papi Rogelio, por su cariño, compresión e incondicional apoyo, por su esfuerzo por darme los recursos necesarios para mi educación, por creer en mí. Gracias por todo en mis estudios y gracias también por haberme enseñado a jugar fútbol.

A mi hermanita Lizbeth, por ser mi mayor ejemplo a seguir, por haberme enseñado el significado de la palabra perseverancia y esfuerzo, por brindarme su cariño y apoyo.

A mi hermanito Rodrigo, porque con su llegada Dios le dio a mi familia la bendición más grande, porque con su llegada todo empezó a ser mejor, porque de él aprendí a sonreír pase lo que pase. Hermanito algún día cuando leas esta dedicatoria recuerda esto, tú serás mejor que yo y siempre me sentiré orgulloso de ti.

A mi hijo Leo, porque Dios me bendijo nuevamente y sobre todo porque con él entendí que la vida puede ser aún mejor. Hijo quiero que sepas que guiaré tus pasos para que llegues a ser un buen profesional pero sobre todo una mejor persona.

Dedico este trabajo a todos ellos(as), pilares fundamentales en mi vida; sin ellos, jamás hubiese llegado a ser lo que hoy soy.

ÍNDICE

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tuvo por objetivo "Describir el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes S.A. en el periodo Diciembre 2014 a Diciembre 2015", para ello el tipo de investigación utilizado fue no experimental con diseño descriptivo, la población de estudio fue constituido por todo el personal de la Caja Rural de Ahorro y Crédito Los Andes S.A., con un tipo de muestra no probabilístico intencional determinado de acuerdo a la experiencia del investigador. Asimismo, con el propósito de describir la Gestión de Riesgos de Tecnología de Información se utilizó la encuesta del Modelo de Madurez establecida, la cual nos dio a conocer el nivel de madurez de la Gestión de Riesgos de Tecnología de Información en los periodos Diciembre 2014 a Diciembre 2015, dichas encuestas fueron completadas en base a la observación del investigador y en base a la intervención de todos los involucrados en los procesos de Tecnología de Información de la Caja Rural de Ahorro y Crédito Los Andes S.A. Finalmente, se concluyó que el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en el periodo Diciembre 2014 fue Inicial (Nivel 1) y en el periodo Diciembre 2015 fue Definido (Nivel 3), dichos niveles de madurez son descritos en el capítulo IV sección 4.2 del presente documento.

PALABRAS CLAVE: Gestión de Riesgos de Tecnología de Información, Marco de Trabajo RISK IT, Modelo de Madurez.

ABSTRACT

The objective of this research was to "Describe the maturity level of the application of the RISK IT Framework in the IT Risk Management in the Caja Rural de Ahorro y Credito Los Andes S.A. in the period December 2014 to December 2015", for this the type of research used was non-experimental with descriptive design, the study population was constituted by all the staff of the Caja Rural de Ahorro y Credito Los Andes S.A., with an intentional non-probabilistic sample type determined according to the researcher's experience. Likewise, with the purpose of describe the IT Risk Management was used the survey of the Maturity Model established, which made us known the maturity level of IT Risk Management in the period December 2014 to December 2015, these surveys were completed based on the observation of the researcher and based on the intervention of all those involved in the processes of Information Technology of the Caja Rural de Ahorro y Credito Los Andes S.A. Finally, it was concluded that the maturity level of the application of the RISK IT Framework in the IT Risk Management in the period December 2014 was Initial (Level 1) and in the period December 2015 was Definite (Level 3), these levels of maturity are described in the chapter IV section 4.2 of this document.

KEYWORDS: IT Risk Management, RISK IT Framework, Maturity Model.

INTRODUCCIÓN

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

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

Con el afán de hacer frente a este tipo de riesgo, se han incorporado distintas normativas y buenas prácticas que buscan evitar pérdidas para la organización a través de la gestión continua de los riesgos de TI.

Para la presente investigación se han descrito los resultados de la aplicación del Marco de Trabajo RISK IT, el cual es propiedad de ISACA (organización internacional dedicada al control del gobierno corporativo), dichos resultados han sido interpretados a través del Modelo de Madurez utilizado para su evaluación en la Caja Rural de Ahorro y Crédito “Los Andes” S.A.

Asimismo, la presente tesis está organizada en cuatro capítulos, además de las conclusiones y sugerencias.

En el **Capítulo I** se describe el planteamiento del problema de investigación, y además la justificación y objetivos de la investigación.

En el **Capítulo II** se describen los antecedentes basados en trabajos de investigación similares, así como los aspectos teóricos en los que se basa esta investigación; en este capítulo también se plantea la hipótesis de la investigación así como la operacionalización de variables.

En el **Capítulo III** se describe el diseño metodológico, la población y la muestra de la investigación, así como las técnicas e instrumentos utilizados para la recolección de datos.

Finalmente, en el **Capítulo IV** se analizan e interpretan los resultados obtenidos, asimismo se dan a conocer las conclusiones y sugerencias para la presente investigación.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

Hoy en día la mayoría de las empresas soportan sus procesos operativos con TI, se ha generado un alto grado de dependencia de las tecnologías de información, las organizaciones en general tienen una elevada inversión en tecnología, puesto que el no hacerlo ocasiona perder competitividad en el mercado, lo cual se traduce en pérdidas.

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

Sin embargo, toda oportunidad conlleva riesgos de diferente índole y dependiendo de las circunstancias en las que ocurran, estos riesgos pueden afectar de una o de otra forma los resultados que las empresas desean obtener, "según estudio recogido por PricewaterhouseCoopers, un 75% de los empresarios cree que los riesgos están creciendo cada día, es decir, se están presentado más riesgos en las organizaciones" (Young, 2014).

Existen distintos tipos de riesgos que se presentan en las empresas del sistema financiero, dentro de los cuales se encuentran el riesgo crediticio, el riesgo operacional, el riesgo de mercado, el riesgo de liquidez, el riesgo estratégico y el riesgo reputacional; adicionalmente a los mencionados se contemplan los riesgos de tecnologías de información, los mismos que vienen cobrando mayor relevancia con el pasar del tiempo; Young (2014) considera que: "El evento que se está presentado que hace que las compañías sientan que hay más riesgos para hacer negocios son los cambios tecnológicos y los riesgos en tecnologías

de información (TI)", es por ello que todas las empresas, y sobre todo las que se encuentran en el sector financiero deben administrar adecuadamente el riesgo mencionado a fin de evitar incidentes que pueden impactar negativamente y causar daños o pérdidas en diferentes grados de severidad.

Caja Rural de Ahorro y Créditos "Los Andes" S.A. es una empresa dedicada a brindar servicios micro financieros, la misma que gestiona sus riesgos de manera integral, teniendo en el riesgo operacional uno de sus pilares fundamentales, dentro del cual se encuentra como un factor que forma parte de su composición el análisis de riesgos de tecnologías de información, dicho análisis podría haberse realizado de manera superficial, por lo que los riesgos podían no identificarse, los niveles de los riesgos podían evaluarse de manera errónea o no evaluarse y asimismo podían no establecerse planes de tratamiento efectivos que mitiguen los riesgos; ello conllevaría además a que el personal que laboraba en la institución no tenga conocimiento de la labor que se debería realizar en cuanto a la gestión de riesgos de tecnologías de información, por lo tanto ello ocasionaba que no tengan idea de las consecuencias de no gestionar el riesgo en mención; asimismo si la empresa no brindaba los recursos necesarios para dicha gestión o si no se le prestaba la debida atención, en algún momento sus altos directivos podrían haberse dado cuenta de los riesgos que la empresa enfrentaba y pudo ser demasiado tarde, puesto que ello podría haber ocasionado la interrupción de sus servicios de manera temporal o incluso el cierre total de la empresa llevándola a la quiebra.

1.1.1. DEFINICIÓN DEL PROBLEMA

1.1.1.1. PROBLEMA GENERAL

¿Cuál es el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?

1.1.1.2. PROBLEMAS ESPECÍFICOS

a) ¿Cuál es el nivel de madurez del dominio "Gobierno del Riesgo" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?

b) ¿Cuál es el nivel de madurez del dominio "Evaluación de Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?

c) ¿Cuál es el nivel de madurez del dominio "Respuesta a los Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?

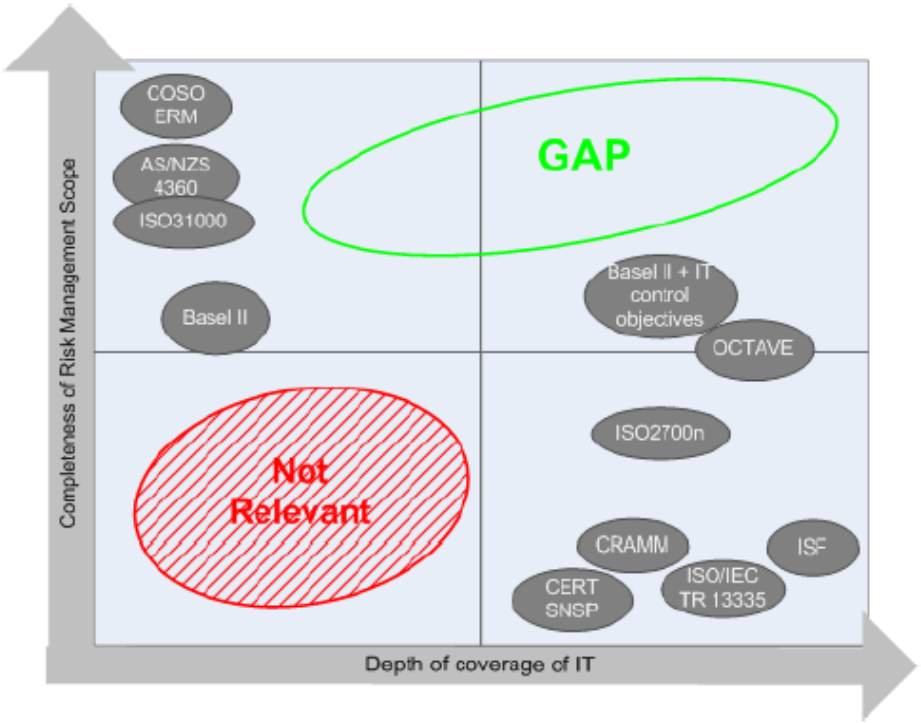
1.2. JUSTIFICACIÓN DEL PROBLEMA

En el sector financiero así como en distintas industrias cada día hay más empresas que entienden la importancia de gestionar los riesgos de tecnologías de información, si bien los riesgos se presentan como amenazas y se generan a partir de vulnerabilidades, los riesgos

son inciertos, no se sabe en qué momento podrían materializarse, por lo tanto deben ser gestionados oportunamente y bajo una metodología adecuada.

Para cubrir dicha necesidad, se han presentado varias metodologías y marcos de referencia, los cuales buscan ofrecer un conjunto de prácticas avaladas por la industria, con el objetivo de que las empresas aterricen u optimicen sus procesos de gestión de riesgos, sin embargo, los marcos de referencia comúnmente empleados son genéricos, dejando una brecha en el cubrimiento del proceso tal como lo ilustra la Figura 1.

Figura 1: RISK IT Framework for Management of IT Related Business Risks



Fuente: (ISACA, 2009)

En la presente investigación se describió la aplicación del marco de trabajo RISK IT, el cual provee un proceso de principio a fin para la administración exitosa del riesgo de tecnologías de información, asimismo brinda las mejores prácticas con el fin de establecer

un marco de trabajo para las organizaciones. Este marco de referencia brinda una guía para realizar la gestión de riesgos a través de la identificación, evaluación y tratamiento, ampliando la visión de este proceso a un contexto más extenso basándose en el valor y en los beneficios que la organización obtiene a través de las iniciativas de TI, está conectada a los objetivos del negocio, alinea la gestión de los riesgos de TI con la gestión de riesgos corporativa, balancea los costos y beneficios de la administración de los riesgos y finalmente genera un gobierno efectivo de TI a nivel corporativo.

Fischer (2010) afirma que:

> El marco de trabajo RISK IT reduce costes, esfuerzo y tiempo proporcionando una metodología clara enfocada en los riesgos de los negocios basada en TI como la finalización tardía de proyectos, cumplimiento normativo y legal, desalineamiento, arquitectura obsoleta de TI, problemas en la entrega de servicios, entre otros; asimismo indica que el marco de trabajo RISK IT provee una guía para los ejecutivos y gestores a centrarse en las preguntas clave, tomar mejores decisiones ajustadas a sus riesgos y dirigir sus organizaciones a gestionar los riesgos de forma eficiente.

La investigación aquí planteada fue pertinente, porque permitió a la CRAC “Los Andes” S.A. tener mayor competitividad y éxito en el logro de sus objetivos, maximizando sus ganancias y haciendo que sus procesos de soporte asociados a las tecnologías de información sean más eficaces y eficientes, asimismo la investigación fue de interés para todo el personal, siendo aún más importante para la plana gerencial y los inversionistas de la compañía, puesto que la presente viene otorgando mayor sostenibilidad en el negocio y generando una visión a largo plazo.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. OBJETIVO GENERAL

Describir el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.

1.3.2. OBJETIVOS ESPECÍFICOS

a) Analizar el nivel de madurez del dominio "Gobierno del Riesgo" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.

b) Analizar el nivel de madurez del dominio "Evaluación de Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.

c) Analizar el nivel de madurez del dominio "Respuesta a los Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

- **TESIS: Plan de Acción para Minimizar la Exposición al Riesgo Tecnológico de una PYME basada en el Marco de Referencia RISK IT**, desarrollado por (Gualim Ac, 2014) en la Universidad de San Carlos de Guatemala para la obtención del título de Ingeniero de Ciencias y Sistemas, en cuyo objetivo indica:

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

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

- **TESIS: RISK IT como complemento a la Gestión de Riesgos en compañías de la industria de Software**, desarrollado por (Montenegro Hoyos & Riveras, 2011) en la Universidad ICESI de Colombia para la obtención del título de Magister en Gestión de Informática y Telecomunicaciones con énfasis en Gerencia de Tecnologías de Información y Telecomunicaciones, en cuyo objetivo indica:

  Generar un conjunto de recomendaciones para gestionar los riesgos de TI en empresas ya valoradas con el modelo CMMI de manera escalonada a partir del nivel 3 o superior con la implementación del área de procesos para gestión de riesgos RSKM

empleando el marco de referencia para gestión de riesgos RISK IT de ISACA con el fin de generar una guía de mejores prácticas que permitan a estas empresas implementar o reforzar el proceso de gestión de riesgos.

La investigación evidenció que los proyectos de desarrollo de software y en general la industria de software, es de alto riesgo y de ahí la importancia de definir y realizar un proceso adecuado para gestión de los mismos. Asimismo, la investigación permitió identificar que las empresas en sus procesos formales de gestión de riesgos no contemplan la identificación de los riesgos positivos, ni la identificación de las oportunidades existentes en el mercado, los cuales se podrían traducir de manera controlada en la generación de valor para sus negocios.

- **TESIS: Gestión de Riesgos Corporativos de TI en Guatemala**, desarrollado por (López Marcos, 2011) en la Universidad de San Carlos de Guatemala para la obtención del título de Ingeniero en Ciencias y Sistemas, en cuyo objetivo indica:

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

A partir de la investigación realizada se concluye que la gestión de riesgos de TI en las organizaciones sirve para evitar y minimizar pérdidas, pero también es útil para generar valor por medio de la aplicación de conceptos, principios y un conjunto de acciones definidas en controles, las cuales se definen como respuestas a estos riesgos, los cuales involucran la implementación del proceso de mejora continua del nivel de madurez.

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

- **TESIS: Metodología de Evaluación del Riesgo Tecnológico en las Instituciones del Sistema Financiero Ecuatoriano, Utilizando COBIT 4.1**, desarrollado por (Coronel Hoyos, 2008) en la Universidad de las Fuerzas Armadas de Ecuador para la obtención del título de Ingeniero de Sistemas e Informática, en cuyo objetivo indica:

  Desarrollar una metodología de evaluación del riesgo tecnológico para las instituciones financieras controladas por la Superintendencia de Bancos y Seguros del Ecuador, utilizando el marco de trabajo de COBIT 4.1.

  La investigación concluye indicando que las etapas y actividades planteadas para la metodología de evaluación del riesgo tecnológico, permitieron alcanzar los objetivos propuestos, asimismo el plan piloto en el que se aplicó la metodología propuesta para la evaluación del riesgo tecnológico, permitió determinar que de su aplicación se obtienen resultados consistentes con la realidad de la institución evaluada, utilizando una de las mejores prácticas en administración de la tecnología de información, como lo es el marco de trabajo COBIT.

2.2. SUSTENTO TEÓRICO

2.2.1. RIESGOS

2.2.1.1. CONCEPTO

Si bien la antigüedad del concepto "riesgo" (bajo la idea de un "porvenir sin certeza") se ha hecho manifiesto, su definición resulta ser una tarea compleja, ya que ésta no sólo ha sufrido diferentes adaptaciones conceptuales en diferentes momentos de la historia, sino que cambia conforme a la disciplina y el enfoque desde el cual se le aborde. Por esto, y a pesar del tupido volumen de investigaciones, reflexiones y literatura al respecto, la mayor parte de los estudios concuerdan en afirmar que el origen de la palabra "riesgo" es desconocido y no cuenta con una definición homogénea, libre de cualquier problematización.

Desde una mirada terminológica, es prudente precisar que en español el término hace referencia a dos significados que, en inglés, corresponden a dos significantes diferentes: risk y hazard; los cuales se usan, algunas veces, de forma indistinta tanto en el lenguaje científico como, principalmente, en el lenguaje cotidiano. Lo que en inglés se denomina risk, en español equivale al término "riesgo", indicando con ello posibilidad en el sentido de probabilidad de daños o pérdidas. Pero a la vez, "riesgo" también se utiliza en español para designar la fuente de esos posibles daños (hazard en inglés), es decir, para denotar actividades, tecnologías, sustancias o acontecimientos capaces de producir afectaciones (Puy, 1995).

(Kaplan & Garrick, 1981), al abordar los aspectos cualitativos que atraviesan la noción de riesgo, puntualizan muy bien esta distinción entre hazard y risk. El primero es entendido como fuente de peligro, mientras el segundo como la posibilidad o el grado de probabilidad de daño. En este mismo sentido, en el Diccionario de la Real Academia Española (2001) se encuentran

dos acepciones de “peligro”: una como sinónimo de riesgo, en el sentido probabilístico ya referido, esto es: “riesgo o contingencia inminente de que suceda algún mal”; y otra poniendo más énfasis en la fuente de ese daño, esto es: “lugar, paso, obstáculo o situación en que aumenta la inminencia del daño”.

A continuación se definen tres conceptos de riesgos en las organizaciones:

Según Fernando Izquierdo Duarte: “El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos”.

Según Alberto Cancelado González: “El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas”.

Según Martín Vilches Troncoso: “El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio. Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado”.

Por lo tanto el riesgo se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y probabilidad de ocurrencia.

2.2.1.2. CLASIFICACIÓN DE LOS RIESGOS

Los riesgos pueden surgir por diversas fuentes, internas o externas, y pueden agruparse en diversas categorías o tipos. La Superintendencia de Banca Seguros y Administradora de

Fondo de Pensiones (SBS) en su Resolución SBS N° 0037-2008 enumera una lista no limitativa de los diversos tipos de riesgos a que está expuesta una empresa, las mismas que se enumeran en el siguiente apartado:

- **RIESGO DE CRÉDITO**

La posibilidad de pérdidas por la incapacidad o falta de voluntad de los deudores, contrapartes, o terceros obligados, para cumplir sus obligaciones contractuales registradas dentro o fuera del balance.

- **RIESGO ESTRATÉGICO**

La posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

- **RIESGO DE LIQUIDEZ**

La posibilidad de pérdidas por incumplir con los requerimientos de financiamiento y de aplicación de fondos que surgen de los descalces de flujos de efectivo, así como por no poder cerrar rápidamente posiciones abiertas, en la cantidad suficiente y a un precio razonable.

- **RIESGO DE MERCADO**

La posibilidad de pérdidas en posiciones dentro y fuera de balance derivadas de fluctuaciones en los precios de mercado.

- **RIESGO OPERACIONAL**

La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

- **RIESGO DE SEGURO**

La posibilidad de pérdidas por las bases técnicas o actuariales empleadas en el cálculo de las primas y de las reservas técnicas de los seguros, insuficiencia de la cobertura de reaseguros, así como el aumento inesperado de los gastos y de la distribución en el tiempo de los siniestros. Se le conoce también como riesgo técnico.

- **RIESGO DE REPUTACIÓN**

La posibilidad de pérdidas por la disminución en la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.

2.2.1.3. TIPOS DE CAUSAS DE RIESGOS

Las causas de riesgo más comunes, para efectos del tema, se dividen en:

- Externas e
- Internas.

Las causas de riesgo externas pueden ser de dos clases:

- Naturales y
- Motivadas por el Hombre.

Las causas de riesgo naturales son normalmente las siguientes:

- Inundaciones.
- Temblores.
- Tornados.
- Tormentas Eléctricas.
- Huracanes.
- Erupciones Volcánicas.

Las causas de riesgo originadas por el hombre, son entre otras, las siguientes:

- Incendios.
- Explosiones.
- Accidentes laborales.
- Destrucción intencional.
- Sabotaje.
- Robo.
- Fraude.
- Contaminación Ambiental.

Las causas internas de riesgo, se generan a partir de las mismas empresas. Son más frecuentes las causas internas de riesgo que las causas externas. Entre las causas internas de riesgo tenemos básicamente:

- Robo: de materiales, de dinero y de información.
- Sabotaje.
- Insuficiencia de Dinero.
- Destrucción: de datos y de recursos.
- Personal No capacitado.

- Huelgas.
- Fraudes.
- Ausencia de seguridades físicas tanto de la empresa como de la información.

2.2.2. RIESGO DE TECNOLOGÍAS DE INFORMACIÓN

2.2.2.1. CONCEPTO

El Riesgo de Tecnologías de Información es la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información que la empresa dispone para prestar sus servicios.

Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión.

El concepto de riesgo de TI puede definirse también como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Es el control el que actúa sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

ISACA (2009) afirma:

"Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos." (p. 11)

En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo, por ejemplo, el sector financiero en el marco de Basilea II. Sin embargo, incluso el riesgo estratégico de TI puede tener un componente financiero, especialmente en aquellas organizaciones en las que es el elemento clave de nuevas iniciativas empresariales. Lo mismo se aplica para el riesgo de crédito, donde una política pobre en cuanto a seguridad de la información se refiere, puede conducir a menores calificaciones de crédito. Por esta razón, es mejor no describir los riesgos de TI con una dependencia jerárquica en una de las categorías de riesgo, tal como se muestra en el ejemplo orientado a la industria financiera de la Figura 2.

Figura 2: Los riesgos de TI como un componente del universo de riesgos

Fuente: (ISACA, 2009)

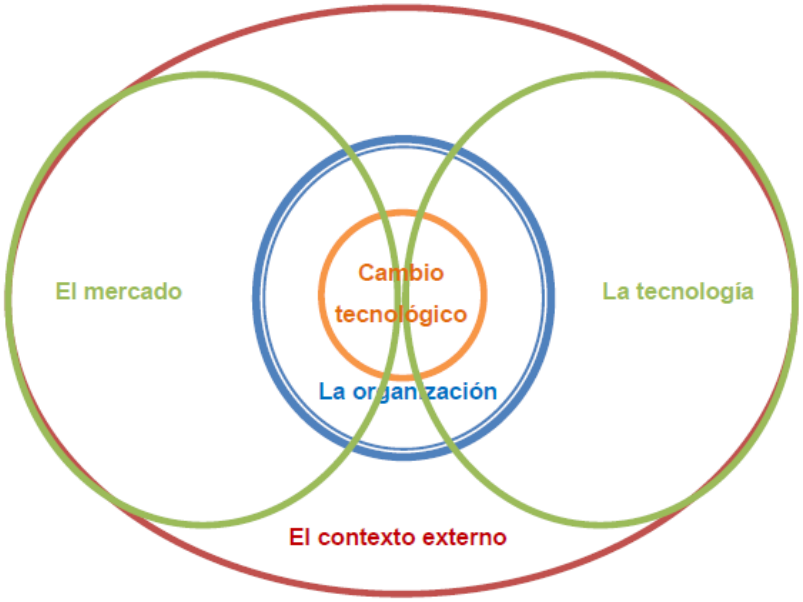
2.2.2.2. ORIGEN DEL RIESGO DE TI

Considerando que los riesgos que se encuentran asociados a la tecnología, desde su concepción, desarrollo y utilización, los cuales no solo impactan a las organizaciones que las

conciben durante su periodo de desarrollo; los orígenes pueden ser diversos, de los cuales, los más frecuentes según Antonio Hidalgo Nuchera, son:

- Derivado del proceso de adquisición o transferencia de tecnología: regularmente estos son ocasionados por razones internas originadas de planificaciones deficientes o son ocasionados por la falta de adaptación de los recursos humanos que se encuentran implicados en el proceso.
- Originados por dificultades en la organización receptora: son causas que tienen su origen en la organización que dará uso a la TI y que afectan el desarrollo o implantación.
- Derivadas de la tecnología utilizada para su desarrollo: regularmente son originados por el uso de una tecnología inestable o que se vuelve obsoleta.
- Derivadas de factores externos a la organización: corresponden a factores fuera del alcance de la organización que imposibilitan el acceso a la tecnología, su mantenimiento o soporte para continuar con su uso, cuyos factores pueden estar relacionados a causas socioeconómicas o políticas, entre otras.
- Derivadas del mercado y su evolución durante el desarrollo de la tecnología: se encuentran relacionadas a acontecimientos no previstos que pueden impactar directamente en los resultados esperados durante el desarrollo de la tecnología; se encuentran relacionados a aspectos económicos y de penetración tecnológica que a pesar de no estar ligados a las TI, les impacta desfavorablemente, como por ejemplo, una crisis económica global, recesión económica y caídas del valor del dinero.

Figura 3: Fuentes de Riesgo



Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

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

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

2.2.2.3. IMPACTO DEL RIESGO DE TI

Durante muchos años el impacto del riesgo tecnológico fue asociado solamente a las áreas de tecnología siendo estas los responsables de cada uno de los incidentes que ocurrían si en algún momento se llegaban a materializar los escenarios de riesgo, es por ello que la evaluación de riesgos de TI, así como las decisiones que se tomen para su mitigación, deben ser expresadas en términos del negocio de tal forma que estos sean comprensibles por las diferentes partes involucradas (áreas de tecnología y áreas del negocio); debiendo poder comprender y expresar cada una de las áreas del negocio, cómo se ve impactada la empresa si algún riesgo se materializa, generando eventos adversos que impactan a los objetivos estratégicos de la empresa.

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

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

- Criterios de información COBIT: se enfoca en expresar los riesgos de TI en aspectos comerciales, basándose en que el impacto se encuentra en no contar con la información, siendo una descripción intermedia y no una definición del impacto del

negocio. Esta se concentra en definir el impacto a través de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, conformidad y cumplimiento.

- Criterios de Balanced Scorecard - BSC: se enfoca en los objetivos del negocio desde las perspectivas financieras, del cliente, internas y de crecimiento.
- Criterios extendidos BSC: la lógica es similar a la anterior, sin embargo, esta se concentra en bajar a un nivel más específico en donde se consideran los aspectos que impactan al negocio, limitándolo a un conjunto de criterios específicos y tangibles, siendo un método selectivo en donde debe tomarse en consideración que existen relaciones causa efecto entre las diferentes perspectivas. Por ejemplo, la perspectiva financiera medida por valor de la acción, beneficio, ingresos y costo de capital; de clientes medida por market share, satisfacción del cliente y percepción de servicio al cliente; interna medida por el cumplimiento de normativas; de crecimiento medida por ventaja competitiva y reputación.
- Criterios según (Westerman, 2007): el marco 4A, define el riesgo de TI como la posibilidad de acontecimiento imprevisto de un evento que amenaza los objetivos de la empresa relacionados entre sí: agilidad (agility), precisión (accuracy), acceso (access) y disponibilidad (availability).
- Criterios según COSO-ERM: se basa en cuatro categorías de objetivos: estrategia, operaciones, información y cumplimiento; enfocándose en que los objetivos del negocio deben estar alineados a la estrategia, la eficiencia y eficacia operativa garantizando el rendimiento y la rentabilidad, la fiabilidad de la información tanto interna como externa, así como la financiera y no financiera, y la adhesión al cumplimiento de leyes, normativas y reglamentos.

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

2.2.3. GESTIÓN DE RIESGOS

2.2.3.1. CONCEPTO

En la economía global, las organizaciones necesitan tomar riesgos para sobrevivir, la mayoría de ellas necesitan incrementar el nivel de riesgos que toman para ser exitosas a largo plazo. Con el significativo incremento en la competencia, los objetivos y metas agresivos de las corporaciones se están convirtiendo en norma. Para direccionar este cambio, los líderes mundiales están fortaleciendo sustancialmente sus prácticas de gestión de riesgos para asegurar que si las iniciativas o el funcionamiento de las unidades de negocio "se descarrilan", esto se identifique rápidamente poder actuar para corregir la situación.

La Gestión de Riesgos es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

2.2.3.2. BENEFICIOS PARA LA ORGANIZACIÓN

La Gestión de Riesgos dentro de una organización genera beneficios, dentro de los cuales podemos mencionar:

- Facilita el logro de los objetivos de la organización.

- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.

2.2.3.3. FACTORES A CONSIDERAR

Los principales factores que se deben considerar en la Gestión de Riesgos de TI son:

- Seguridades.
- Controles: Preventivos, Detectivos y Correctivos.
- Objetivos.
- Manuales de usuarios.
- Políticas.

Si no existe una adecuada consideración de los factores antes descritos y si nuestros controles y seguridades fueran errados, nuestros planes organizacionales, financieros, administrativos y de sistemas se verían seriamente afectados, ya que no sólo el área de sistemas será el afectado.

2.2.4. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN

2.2.4.1. CONCEPTO

Es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de Tecnologías de Información.

La gestión de riesgos es entonces el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que se deben seguir en las organizaciones para identificar, valorar y manejar los riesgos asociados a los procesos de TI de la organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades de mejora.

2.2.4.2. BENEFICIOS DE LA GESTIÓN DE RIESGOS DE TI

A nivel organizacional:

- Alcance o logro de los objetivos organizacionales.
- Énfasis en prioridades de negocio: permite a los directivos enfocar sus recursos en los objetivos primarios. Tomar acción para prevenir y reducir pérdidas, antes que corregir después de los hechos, es una estrategia efectiva de administración del riesgo.
- Fortalecimiento del proceso de planeación.
- Apoyo en la identificación de oportunidades.
- Fortalecimiento de la cultura de autocontrol.

Al proceso de administración o gestión:

- Cambio cultural que soporta discusiones abiertas sobre riesgos e información potencialmente peligrosa. La nueva cultura tolera equivocaciones pero no tolera errores escondidos. La nueva cultura también hace énfasis en el aprendizaje de los errores.
- Mejor administración financiera y operacional al asegurar que los riesgos sean adecuadamente considerados en el proceso de toma de decisiones. Una mejor

administración operacional generará servicios más efectivos y eficientes. Anticipando los problemas, los directivos tendrán mayor oportunidad de reacción y tomar acciones. La organización será capaz de cumplir con sus promesas de servicio.

- Mayor responsabilidad de los administradores en el corto plazo. A largo plazo, se mejorarán todas las capacidades de los directivos.

2.2.4.3. CARÁCTERÍSTICAS GENERALES DE LA GESTIÓN DE RIESGOS DE TI

La Gestión de Riesgos es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario, cuyas características generales son:

- La Gestión de Riesgos debe estar apoyada por la alta gerencia de la organización.
- La Gestión de Riesgos debe ser parte integral del proceso administrativo utilizado por la dirección de la organización.

2.2.4.4. OBJETIVOS DE LA GESTIÓN DE RIESGOS DE TI

Algunos objetivos importantes de la gestión de riesgos de tecnologías de información en las organizaciones actuales son:

- Mantener seguros los sistemas tecnológicos que almacenan, procesan o transmiten información sensible de nuestras organizaciones.
- Permitir que la Alta Dirección tome decisiones adecuadas que justifiquen las inversiones en tecnología que proteja de riesgos.
- Apoyar a la Alta Dirección en la toma de decisiones sobre nuevos sistemas basándose en evaluaciones objetivas de los riesgos relacionados.
- Optimizar costos por la aplicación de medidas de protección.

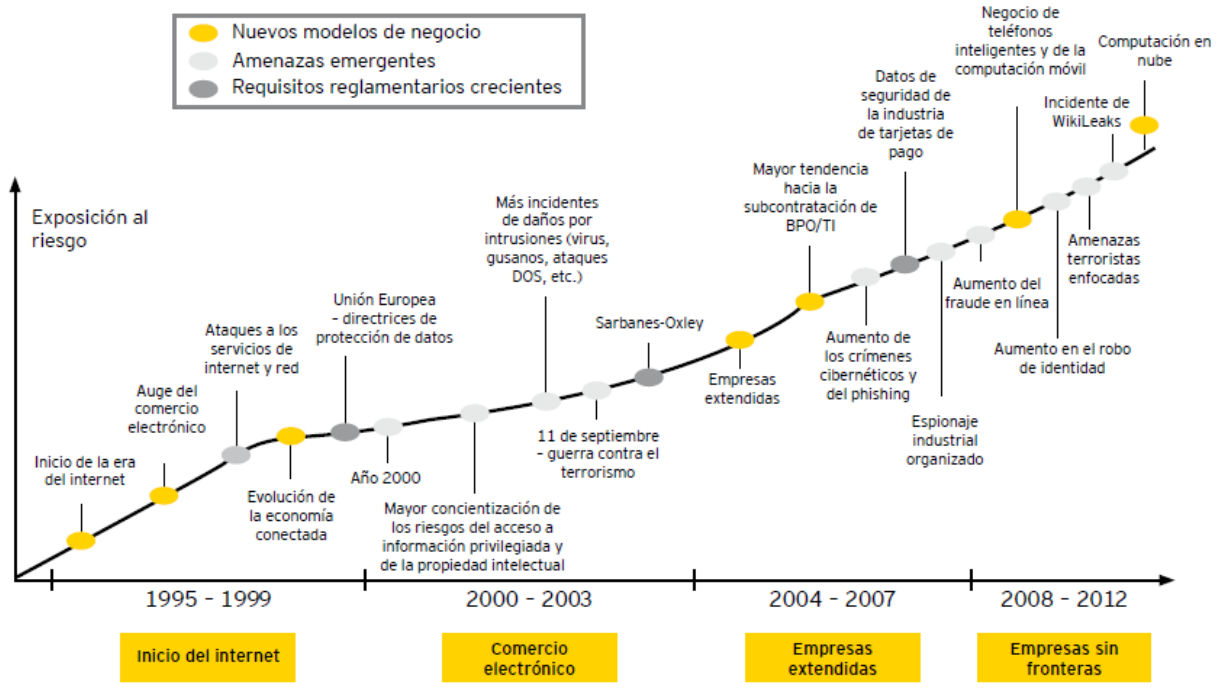
- Evitar pérdidas derivadas de la materialización de los riesgos de tecnologías de información.
- Cumplir con el principio de integridad, puesto que la información debe estar protegida de alteraciones intencionales o accidentales, su ausencia puede resultar en imprecisiones, fraudes o decisiones erróneas.
- Cumplir con el principio de disponibilidad, puesto que la información debe estar siempre lista para ser usada, la falta de disponibilidad puede convertirse en pérdida de tiempo productivo e impedir que los usuarios cumplan adecuadamente sus funciones.
- Cumplir con el principio de confidencialidad, puesto que la información sólo puede ser revelada a personas autorizadas, la falta de confidencialidad puede resultar en pérdida de confianza y reputación o en acciones legales contra la organización

2.2.4.5. IMPORTANCIA QUE COBRA LA GESTIÓN DE RIESGOS DE TI CON EL TIEMPO

La manera en que las compañías interactúan con sus empleados, clientes y otras organizaciones está cambiando a una velocidad sin precedentes. El paradigma de los riesgos de TI siempre ha estado sujeto a cambios, pero la complejidad y los tipos de riesgo han aumentado considerablemente en los últimos años y continuarán incrementándose.

Los modelos cambiantes de negocios, una mayor regulación y los actos intencionales de crímenes cibernéticos aumentan la exposición al riesgo y la necesidad de imponer un nuevo régimen de administración de riesgos. La Figura 4 muestra cómo han cambiado los riesgos con el paso del tiempo.

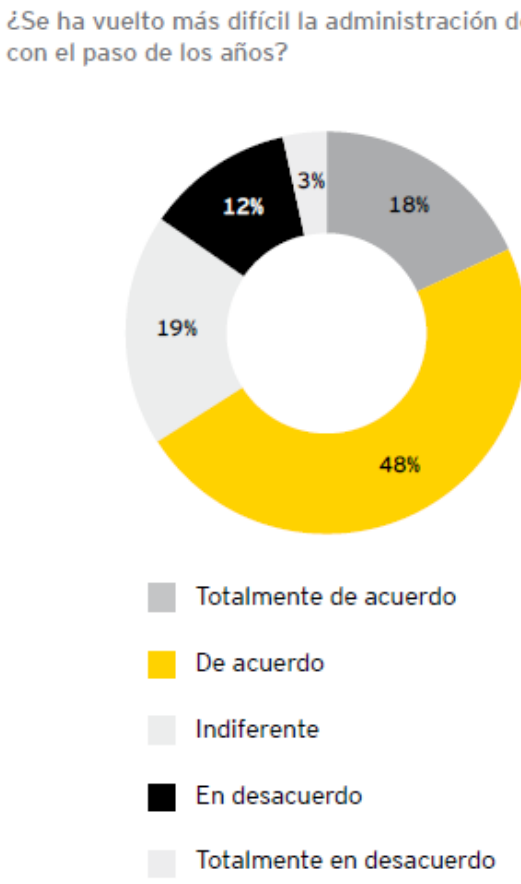
Figura 4: Evolución histórica de los riesgos de TI



Fuente: (Ernst & Young, 2012)

Queda claro que, sin incluir las inquietudes relacionadas con el inicio del nuevo milenio, los riesgos de TI van en aumento. La amplitud y profundidad de los riesgos y la necesidad de contar con contramedidas eficaces se está intensificando de manera rápida, y probablemente continuará aumentando. Muchos negocios están reconociendo esto; en una encuesta realizada, Ernst & Young (2012) afirma que: “dos terceras partes de los encuestados estuvieron de acuerdo en que la administración de riesgos de TI se ha vuelto más desafiante en los últimos años”, ver Figura 5.

Figura 5: Resultados de encuesta a cerca de la administración de Riesgos de TI

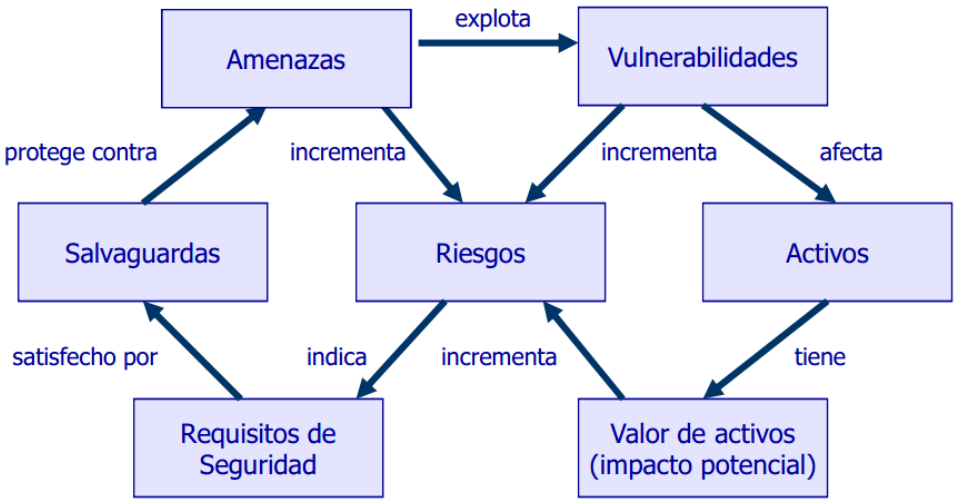


Fuente: (Ernst & Young, 2012)

2.2.4.6. METODOLOGÍAS Y PROCESOS PARA LA GESTIÓN DE RIESGOS DE TI

Existen distintas metodologías y variados procesos para gestionar los riesgos de tecnologías de información, las mismas fueron desarrolladas para la identificación de la falta de controles, el análisis de los niveles de riesgo y el establecimiento de planes de contramedidas. En la Figura 6 se muestran los elementos del análisis de riesgos en forma general.

Figura 6: Elementos del análisis de riesgos



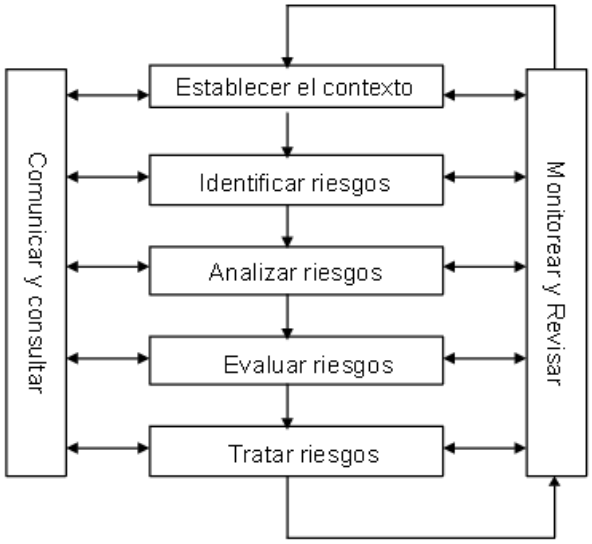
Fuente: (Kaplan & Garrick, 1981)

Es importante también mencionar que para la gestión de riesgos de tecnologías de información existen dos tipos de metodologías: Las cuantitativas y las cualitativas, en este documento citaremos y describiremos los más usados.

A. AS/NZS 4360:2004

Este estándar tiene origen en Australia y Nueva Zelanda, la misma que fue publicada en su primera edición en 1995, en su segunda edición en 1999 y en su tercera edición en 2004. Provee principios y directrices de carácter genérico para la gestión de riesgo corporativo. Se aplica en cualquier tipo de empresa u organización. Está basado en un conjunto de etapas que inician con el establecimiento del contexto del riesgo, con base en ello, se continúa con la identificación, análisis, evaluación y tratamiento de riesgos, tal cual se muestra en la Figura 7.

Figura 7: Vista General de la Gestión de Riesgos



Fuente: (AS, 1999)

A continuación se describen los componentes de la mencionada metodología:

- Establecer el contexto:

El proceso ocurre dentro de la estructura del contexto estratégico, organizacional y de administración de riesgos de una organización. Esto necesita ser establecido para definir los parámetros básicos dentro de los cuales deben administrarse los riesgos y para proveer una guía para las decisiones dentro de estudios de administración de riesgos más detallados. Esto establece el alcance para el resto del proceso de administración de riesgos.

- Identificar riesgos:

Este paso busca identificar los riesgos a administrar. Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización.

- Analizar riesgos:

Los objetivos de análisis son separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.

Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

- Evaluar riesgos:

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

El análisis de riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación de riesgos deberían considerarse sobre la misma base. En consecuencia, la evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario.

El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior. Deberían considerarse los objetivos de la organización y el grado de oportunidad que podrían resultar de tomar el riesgo.

Las decisiones deben tener en cuenta el amplio contexto del riesgo e incluir consideración de la tolerabilidad de los riesgos sostenidos por las partes fuera de la organización que se benefician de ellos.

Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables. Si los riesgos no caen dentro de la categoría de riesgos bajos o aceptables, deberían ser tratados.

- Tratar riesgos:

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

- Monitorear y revisar:

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establece para controlar la implementación. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos.

Es esencial una revisión sobre la marcha para asegurar que el plan de administración se mantiene relevante. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos. La revisión es una parte integral del plan de tratamiento de la administración de riesgos.

- Comunicar y consultar:

La comunicación y consulta son una consideración importante en cada paso del proceso de administración de riesgos. Es importante desarrollar un plan de comunicación para los interesados internos y externos en la etapa más temprana del proceso. Este plan debería encarar aspectos relativos al riesgo en sí mismo y al proceso para administrarlo.

La comunicación y consulta involucra un diálogo en ambas direcciones entre los interesados, con el esfuerzo focalizado en la consulta más que un flujo de información en un sólo sentido del tomador de decisión hacia los interesados.

Es importante la comunicación efectiva interna y externa para asegurar que aquellos responsables por implementar la administración de riesgos, y aquellos con intereses creados comprenden la base sobre la cual se toman las decisiones y por qué se requieren ciertas acciones en particular.

Las percepciones de los riesgos pueden variar debido a diferencias en los supuestos, conceptos, las necesidades, aspectos y preocupaciones de los interesados, según se relacionen con el riesgo o los aspectos bajo discusión. Los interesados probablemente harán juicios de aceptabilidad de los riesgos basados en su percepción de los mismos.

Dado que los interesados pueden tener un impacto significativo en las decisiones tomadas, es importante que sus percepciones de los riesgos, así como, sus percepciones de los beneficios, sean identificadas y documentadas y las razones subyacentes para las mismas comprendidas y tenidas en cuenta.

Algunas de las características adicionales del estándar australiano AS/NZS 4360:2004 son:

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

B. COSO ERM

COSO corresponde a las siglas en inglés del Comité de Organizadores y Patrocinadores de la Comisión Treadway, organismos que en conjunto emitieron el informe con recomendaciones referentes al Control Interno que lleva su nombre.

Su origen viene del año 1985 en Estados Unidos, cuando se forma una comisión patrocinada de diversas instituciones, con el objetivo de identificar las causas de la presentación de información financiera en forma fraudulenta o falsificada. En 1987 emite un informe que contenía una serie de recomendaciones en relación al control interno de cualquier empresa u organización. La comisión Treadway, debatió durante más de cinco años y finalmente en 1992, se emite el informe COSO, el cual tuvo gran aceptación y difusión en gran parte debido a la diversidad y autoridad que posee el grupo que se hizo cargo de la elaboración del informe. COSO ofrece un marco de trabajo integrado que define el control interno en cinco elementos interrelacionados, tal cual se muestra en la Figura 8.

Figura 8: Marco conceptual integrado COSO I

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 1992)

Hacia fines de Septiembre de 2004, como respuesta a una serie de escándalos, e irregularidades que provocaron pérdidas importantes a inversionistas, empleados y otros grupos de interés, nuevamente el Comité de Organizadores y Patrocinadores de la Comisión Treadway, publicó el Enterprise Risk Management - Integrated Framework (COSO II) y sus aplicaciones técnicas asociadas, el cual amplía el concepto de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral del riesgo. Este nuevo enfoque no sustituye el marco de control interno, sino que lo incorpora como parte de él, permitiendo a las compañías mejorar sus prácticas de control interno o decidir encaminarse hacia un proceso más completo de gestión de riesgo. COSO ERM o también conocido como COSO II ofrece un marco de trabajo basado en 8 componentes, los cuales están interrelacionados entre sí, dichos componentes están alineados con 4 objetivos y además se

consideran las actividades en todos los niveles de la organización, como se muestra en la Figura 9.

Figura 9: Marco conceptual integrado COSO ERM

Fuente: (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

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

- Se enfoca en el cumplimiento de los objetivos de negocio.
- Minimiza las sorpresas y pérdidas operativas.
- Identifica y gestiona los riesgos para toda la organización.

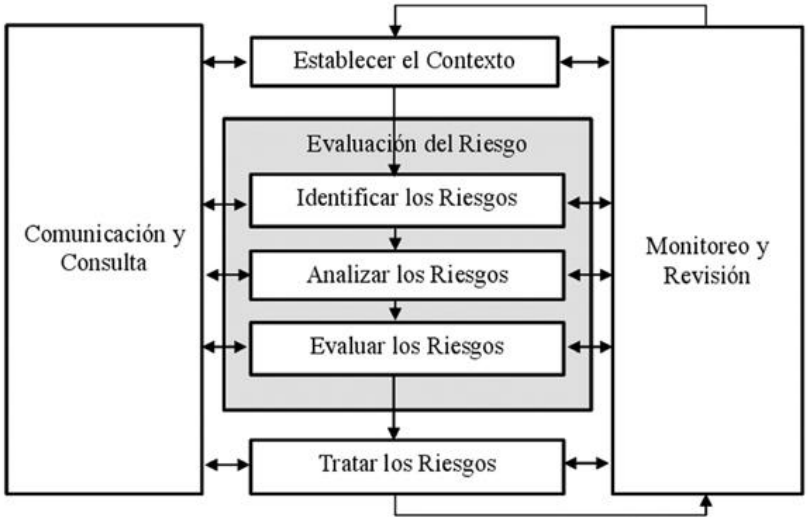
- Fomenta ser proactivo y aprovechar las oportunidades generadas.
- Requiere establecer directrices descendentemente desde la parte superior organizacional hasta los niveles del personal operativo.
- El marco de trabajo está disponible al público por medio de pago.

C. ISO/DIS 31000

Mientras todas las organizaciones gestionan el riesgo a diferentes niveles, esta norma internacional establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz. ISO 31000 recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización.

Esta norma internacional proporciona los principios y las directrices genéricas sobre la gestión del riesgo, puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, no es específica de una industria o sector concreto. En la Figura 10 se muestra su estructura y sus componentes.

Figura 10: Enfoque general del proceso de gestión de riesgos en ENT 5254 e ISO 31000



Fuente: (ISO 31000:2009, 2009)

Algunas de sus características adicionales son:

- Se alinea con los objetivos de negocio.
- Permite su aplicación a lo largo de la vida de una organización
- Es aplicable a cualquier tipo de riesgo, sin diferenciar su naturaleza, así como si tiene efecto positivo o negativo para la organización.
- Requiere establecer directrices descendentemente desde la parte superior en la estructura organizacional hasta el personal operativo.
- Provee un modelo de proceso detallado.

D. OCTAVE

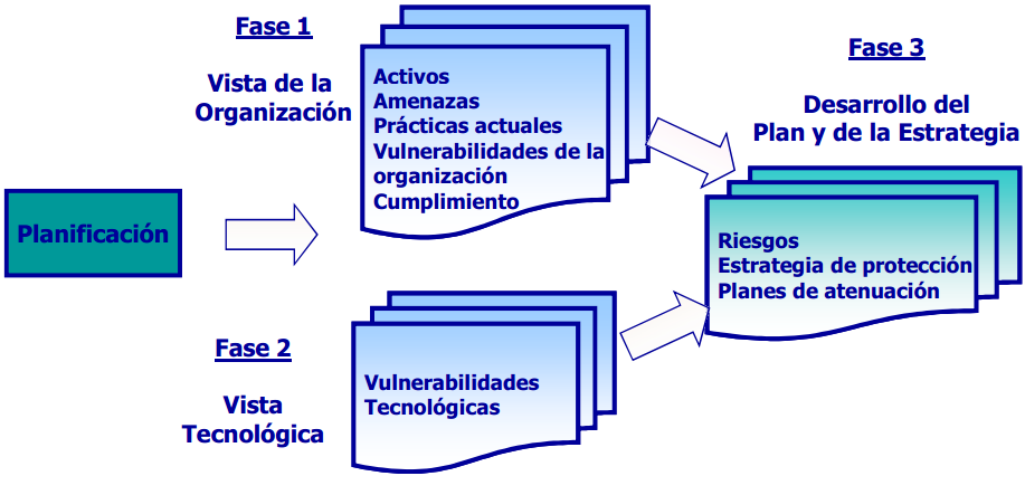
Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) es una metodología para el análisis de riesgos de tecnologías de información, cuyas siglas en español significan: “Evaluación de amenazas operacionalmente críticas, de activos y vulnerabilidades”.

OCTAVE está enfocado a que las organizaciones sean capaces de dirigir y gestionar sus evaluaciones de riesgos, tomar decisiones basándose en sus riesgos, proteger los activos claves de información y comunicar de forma efectiva la información clave de seguridad.

La metodología en mención es también un coadyuvante en el aseguramiento de la continuidad del negocio, define los riesgos y amenazas basadas en los activos críticos, contempla estrategias de protección y mitigación de riesgos basada en prácticas, enfoca la recopilación de datos en función de los objetivos, finalmente OCTAVE podría considerarse como la base para la mejora de la seguridad de la información de las organizaciones que adopten la presente metodología.

Su proceso de administración se muestra en la Figura 11.

Figura 11: Fases de proceso OCTAVE



Fuente: (Kaplan & Garrick, 1981)

A continuación se mencionan algunos beneficios de OCTAVE para las organizaciones:

- Identifica los riesgos de la seguridad que pueden impedir la consecución del objetivo de la organización.

- Enseña a evaluar los riesgos de la seguridad de la información.
- Crea una estrategia de protección con el objetivo de reducir los riesgos de seguridad de la información prioritaria.
- Ayuda a la organización cumplir regulaciones de la seguridad de la información.

E. MAGERIT 2

Es una metodología de análisis y gestión de riesgos de tecnologías de información, la misma que "se ha elaborado como respuesta a la percepción de que la administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos" según explica (Amutio Gómez, Candau, & Mañas, 2012); tiene varios documentos dentro de los cuales se encuentran su método, catálogo y técnicas, asimismo cuenta con una herramienta computarizada denominada "PILAR". Algunas de sus características son:

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

Su esquema completo consta de cuatro fases:

- Planificación del Proyecto de Riesgos

  Se realizan las estimaciones iniciales de los riesgos que pueden afectar al sistema de información así como del tiempo y los recursos que su tratamiento conllevará.

- Análisis de Riesgos

Se estima el impacto que tendrán los riesgos en la organización, cuestión muy importante, puesto que si bien la seguridad es fundamental, su uso desproporcionado puede afectar gravemente al rendimiento del sistema por lo que es necesario establecer un umbral de riesgo deseable (tolerable) que debe superar un determinado riesgo para ser objeto de tratamiento.

- Gestión de Riesgos

  En esta fase se seleccionan posibles soluciones para cada riesgo, en este apartado son fundamentales las prácticas de simulación.

- Selección de Salvaguardas

  Se seleccionan los mecanismos que implementarán las soluciones seleccionadas en la fase anterior.

El esquema del proceso completo de aplicación de la metodología MAGERIT 2 se muestra en la Figura 12.

Figura 12: Esquema del proceso MAGERIT 2

Fuente: (Amutio Gómez, Candau, & Mañas, 2012)

F. ISO/IEC 27005

El estándar internacional ISO/IEC 27005:2008 describe el sistema de gestión de riesgos de seguridad de la información.

La evaluación del riesgo de las amenazas se realiza en base a la probabilidad e impacto, esto ayuda a la gestión de los riesgos, priorizando cada uno de acuerdo a la consecuencia que pueda generar.

El estándar internacional ISO/IEC 27005:2008 fue diseñado para asistir en la implementación de los estándares ISO/IEC 27001 y ISO/IEC 27002. Los conceptos, modelos, procesos y terminologías descritas en ISO/IEC 27001 y 27002 son importantes para el completo entendimiento e implementación del estándar en mención.

Se aplica en cualquier tipo de empresa u organización. Algunas de sus características son:

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

Su proceso de administración se muestra en la Figura 13.

Figura 13: Esquema de procesos del ISO/IEC 27005

Fuente: (Hildago Nuchera, 2014)

G. MARION

Es un método cuantitativo y se basa en la encuesta anual de miembros de la base de incidentes francesa (C.L.U.S.I.F.). No contempla probabilidades, sino esperanzas matemáticas que son aproximaciones numéricas (valores subjetivos).

MARION utiliza cuestionarios y parámetros correlacionados enfocados a las distintas soluciones de contramedidas, en seis categorías. Las categorías son: seguridad informática general, factores socioeconómicos, concienciación sobre la seguridad de software y materiales, seguridad en explotación y seguridad de desarrollo.

El análisis de riesgos lo hace sobre diez áreas problemáticas. Estas áreas son: riesgos materiales, sabotajes físicos, averías, comunicaciones, errores de desarrollo, errores de explotación, fraude, robo de información, robo de software, problemas de personal.

H. MARCO NORMATIVO DE LA GESTIÓN DE RIESGOS EN EL PERÚ

La Superintendencia de Banca, Seguros y AFP (SBS) es el organismo encargado de la regulación y supervisión del sistema financiero peruano. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SPP, asegurando una correcta gestión de riesgos de parte de todas las entidades financieras reguladas en el Perú, para tal objetivo la SBS ha dispuesto normativas que deben ser cumplidas, las mismas que se describen a continuación:

- Resolución SBS N° 0037-2008:

Reglamento para la Gestión Integral de Riesgos diseñado para identificar potenciales eventos que pueden afectar a las empresas del sistema financiero, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos.

Según el reglamento mencionado la Gestión Integral de Riesgos puede descomponerse en componentes, que se encuentran presentes en diversos grados, según se analice la totalidad de la empresa, una línea de negocio, un proceso o una unidad organizativa. La empresa podrá contar con una descomposición propia, que se adapte a su organización, pero ella debe considerar los principales elementos los cuales son: Ambiente interno, establecimiento de objetivos, identificación de riesgos, evaluación de riesgos, tratamiento, actividades de control, información y comunicación y monitoreo.

- Resolución SBS N° 2116-2009:

Reglamento para la Gestión del Riesgo Operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos.

Dicho reglamento indica que las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

- Circular SBS 139-2009:

Reglamento establecido por la SBS con la finalidad de establecer criterios mínimos para la Gestión de la Continuidad del Negocio, que forma parte de una adecuada Gestión del Riesgo Operacional y por lo tanto de una adecuada Gestión del Riesgo de Tecnologías de la Información, su objetivo es implementar respuestas efectivas para que la operatividad del negocio de las empresas continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

- Circular SBS 140-2009:

Reglamento establecido por la SBS con la finalidad de establecer criterios mínimos para la Gestión de la Seguridad de la Información el cual forma parte de una adecuada Gestión del Riesgo de Tecnologías de la Información, su objetivo principal es que las empresas deban establecer, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI), para lo cual las actividades mínimas a realizar son la definición de una política de

seguridad de la información y la definición e implementación de una metodología de gestión de riesgos que guarde consistencia con la gestión de riesgos operacionales de la empresa.

2.2.5. MARCO DE TRABAJO RISK IT

El marco de los riesgos de TI, RISK IT, se complementa con COBIT, que proporciona un marco integral para el control y la gestión de las organizaciones de soluciones y servicios de TI.

Aunque COBIT establece las mejores prácticas para la gestión de riesgos proporcionando un conjunto de controles para mitigar los riesgos de TI, RISK IT establece las mejores prácticas con el fin de establecer un marco para las organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio.

El marco de riesgos de TI es utilizado para ayudar a implementar el gobierno de TI, y las organizaciones que han adoptado (o están planeando adoptar) COBIT como marco de su gobierno de TI pueden utilizar RISK IT para mejorar la gestión de sus riesgos.

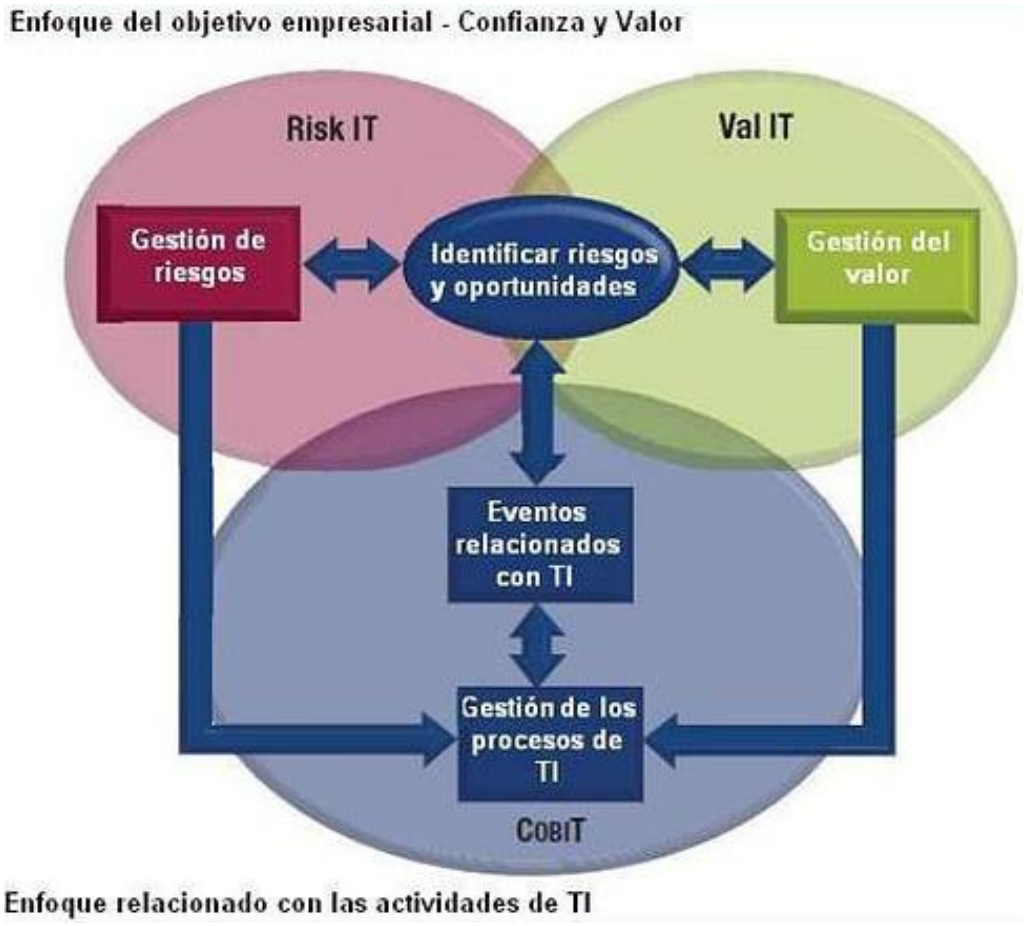
COBIT, propiedad de ISACA, se encarga de gestionar todas las actividades relacionadas con TI en la organización. Estos procesos tienen que tratar con eventos internos o externos a la organización.

Los eventos internos pueden incluir los incidentes operacionales, los fracasos del proyecto, cambios de la estrategia de TI y las fusiones. Los eventos externos pueden incluir cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y las nuevas regulaciones que le afectan.

Estos eventos, plantean un riesgo y una oportunidad para evaluar el mismo y generar las soluciones oportunas. La dimensión del riesgo, y como gestionarlo, es el tema principal de RISK IT. Cuando se identifican las oportunidades de cambios del negocio relacionados con TI, el

Marco VAL IT describe como progresar y maximizar el retorno de la inversión realizada en los mismos. El resultado de la evaluación tendrá probablemente un impacto en algunos de los procesos de TI, por lo que las flechas de la “Gestión de Riesgos" y “Gestión del Valor” se dirigen a la "Gestión de los Procesos de TI", tal y como se muestra en la Figura 14.

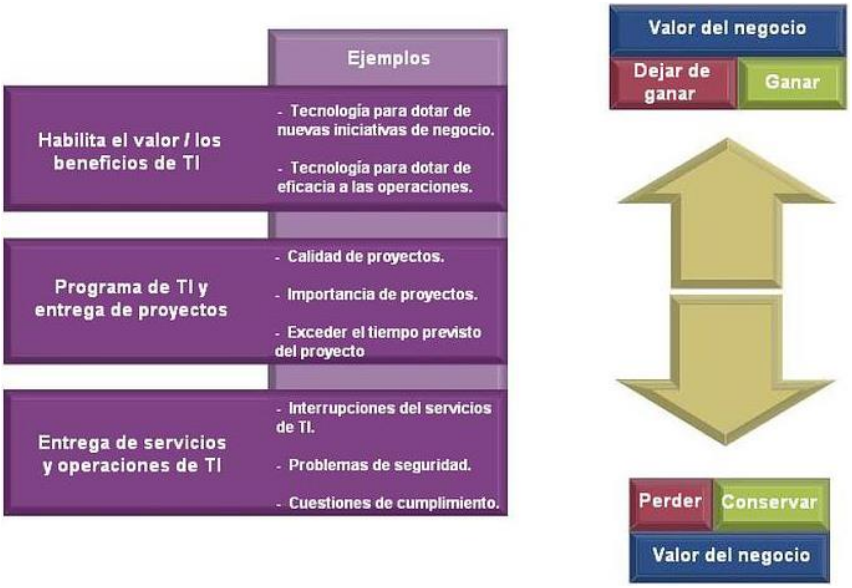
Figura 14: Risk IT, Val IT y COBIT



Fuente: (ISACA, 2009)

Por otro lado, los riesgos de TI pueden clasificarse de diversas maneras, tal cual se muestra en la Figura 15.

Figura 15: Categorías de los riesgos de TI



Fuente: (ISACA, 2009)

2.2.5.1. PROPÓSITO DEL MARCO DE TRABAJO RISK IT

La correcta gestión de los riesgos a los que está expuesta la organización es esencial para la correcta administración de cualquier organización. Casi todas las decisiones de negocio requieren que la alta dirección o los gerentes sopesen los riesgos y los beneficios. El uso común y general de las TI puede proporcionar importantes beneficios a una organización, pero también implica riesgos. Debido a su importancia para las organizaciones, los riesgos relacionados con TI deberían ser tratados como los demás riesgos claves organizacionales, tales como el riesgo del mercado, el riesgo de crédito y otros riesgos operativos. Dichos riesgos los podemos ubicar por debajo de la categoría más crítica de los riesgos en una organización: el hecho de no lograr los objetivos estratégicos del negocio. Si bien estos riesgos han sido incorporados a las organizaciones en los procesos de toma de decisión, muchos ejecutivos tienden a relegar los riesgos a los especialistas técnicos.

El marco de Riesgos de TI explica los riesgos y permite a los usuarios:

- Integrar la gestión de los riesgos en el ERM de la organización, esto permitirá que se tomen decisiones conscientes sobre el retorno de los riesgos.
- Tomar decisiones con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo y la tolerancia al riesgo de la organización.
- Entender cómo responder a los riesgos.

La práctica ha demostrado que la función de TI y los riesgos de TI a menudo no son bien comprendidos por las principales partes interesadas de una organización, entre ellos los miembros de la junta y la dirección ejecutiva. Sin embargo, estas son las personas que dependen de TI para alcanzar los objetivos estratégicos y operativos de la organización y, en consecuencia, deberían ser los responsables de la gestión de los riesgos.

Sin una clara comprensión de la función y de los riesgos asociados a TI, los ejecutivos de alto rango no tienen un marco de referencia para priorizar y administrar los riesgos de TI. Los riesgos de TI no son puramente una cuestión técnica. A pesar de que se necesita de expertos en la materia para entender y gestionar los aspectos de los riesgos de TI, el conocimiento sobre la gestión del negocio es lo más importante. Los gerentes del negocio han de determinar lo que se debe hacer para apoyar su negocio y establecer los objetivos de TI. Por consiguiente, son responsables de la gestión de los riesgos asociados.

El marco de RISK IT proporciona de principio a fin, visión global de todos los riesgos relacionados con el uso de las TI y un tratamiento igualmente minucioso de la gestión del riesgo, desde el tono y la cultura hasta las cuestiones operativas. En resumen, el marco permitirá a las organizaciones entender y gestionar todos los tipos importantes de riesgos de TI. El Marco provee de:

- Un marco de proceso de punta a punta para gestión de riesgos de TI correcta.
- Orientación para los profesionales, incluyendo herramientas y técnicas para entender y gestionar los riesgos concretos para las operaciones de negocio. Esto incluye una lista genérica de campo común, los panoramas relacionados con la TI potencialmente adversos del riesgo que podrían afectar la realización de los objetivos de negocio.

2.2.5.2. EL PÚBLICO Y LAS PARTES INTERESADAS

El público al que está dirigido el marco de RISK IT es muy amplio, ya que se ofrecen razones y beneficios para usar el marco por cada uno de los grupos en cuestión. Todos los grupos citados en la Figura 16 pueden ser considerados partes interesadas para la gestión de los riesgos de TI.

Figura 16: Público interesado para la gestión de los riesgos de TI y sus ventajas

Papel	Beneficios de/ Razones para usar el marco de riesgos de TI
Junta y Dirección Ejecutiva	Mejor comprensión de sus responsabilidades y funciones con respecto a la gestión de riesgos de TI.
Gestores de Riesgos	Asistencia con la gestión de los riesgos de TI, de acuerdo con la organización generalmente aceptados por los principios de la gestión de riesgos.
Administrador de los riesgos Operacionales	Marco de su vinculación con los riesgos de TI, la identificación de las pérdidas operativas o el desarrollo de los principales indicadores de riesgo.
Dirección de TI	Mejor comprensión de cómo identificar y gestionar los riesgos y la forma de comunicar los riesgos a la toma de decisiones de negocios
Directores de servicios de TI	Mejora de su punto de vista sobre los riesgos relacionados con TI, los cuales deberían encajar en el conjunto global del marco de trabajo de la gestión de riesgos de IT.
Administrador de la continuidad de negocio	La alineación con la organización de gestión de riesgos (desde la evaluación de riesgo es un aspecto clave de su responsabilidad)
Administrador de seguridad de TI	Posicionamiento de los riesgos de seguridad, entre otras categorías de riesgo de IT
CFOs	Obtener una mejor visión de los riesgos relacionados con TI y sus implicaciones financieras
Oficiales del gobierno organizacional	Asistencia con su examen y la supervisión de las responsabilidades de gobierno y otras funciones de gobierno de TI.
Directores ejecutivos	La comprensión y la gestión de los riesgos es uno de los muchos riesgos de negocios, todos los cuales deben ajustarse.
Los auditores de TI	Mejor análisis de riesgo en apoyo de los planes de auditoría e informes
Reguladores	Apoyo de su evaluación de las organizaciones reguladas "enfoque de gestión de riesgos de TI
Auditores externos	Orientación adicional sobre las tecnologías relacionadas con los niveles de riesgo cuando se crea una opinión
Aseguradores	Apoyo en el establecimiento de cobertura de seguro adecuada de TI y la búsqueda de un acuerdo sobre los niveles de riesgo
Las agencias de calificación	En colaboración con aseguradores; una referencia para evaluar objetivamente y la tarifa como una organización se ocupa de los riesgos

Fuente: (ISACA, 2009)

2.2.5.3. BENEFICIOS Y RESULTADOS

El marco de RISK IT aborda muchas cuestiones a las cuales las organizaciones se enfrentan hoy en día, por lo cual es notable su necesidad de:

- Una visión precisa del presente y del futuro próximo sobre los riesgos relacionados con TI en toda la organización y el éxito con el que la organización se ocupa de dichos riesgos.
- Orientación de principio a fin sobre la forma de gestionar los riesgos relacionados con TI, más allá de medidas puramente técnicas de control y de seguridad.
- Comprensión de cómo capitalizar una inversión realizada en un sistema de control interno de TI ya existente para gestionar los riesgos relacionados con TI.
- En cuanto a la evaluación y gestión de los riesgos de TI, la integración con el riesgo global y el cumplimiento de las estructuras dentro de la organización.
- Un marco/lengua común para ayudar a gestionar la relación entre los ejecutivos encargados de adoptar decisiones (o junta de los altos directivos), el director de información (CIO) y la organización de gestión del riesgo, o entre los auditores y la dirección.
- Promoción de la responsabilidad del riesgo y su aceptación en toda la organización.
- Un perfil de riesgo completo para mejor entender el riesgo y aprovechar mejor los recursos de la organización.

2.2.5.4. PRINCIPIOS DE LOS RIESGOS DE TI

RISK IT define, de manera fundamentada, una serie de guías para la gestión eficaz de los riesgos. Dichas guías son generalmente aceptadas sobre la base de los principios de la gestión del riesgo, que se han aplicado en el campo de las TI. El modelo de proceso de RISK IT está

diseñado y estructurado para que las organizaciones puedan aplicar los principios en la práctica y comparar sus resultados.

El marco de RISK IT se refiere a los riesgos de TI, en pocas palabras, los riesgos organizacionales relacionados con el uso de las tecnologías de información. La conexión con el negocio se fundamenta en los principios en los que se basa el marco, por ejemplo, un gobierno efectivo de la organización y la gestión eficaz de los riesgos de TI, tal y como se muestra en la Figura 17.

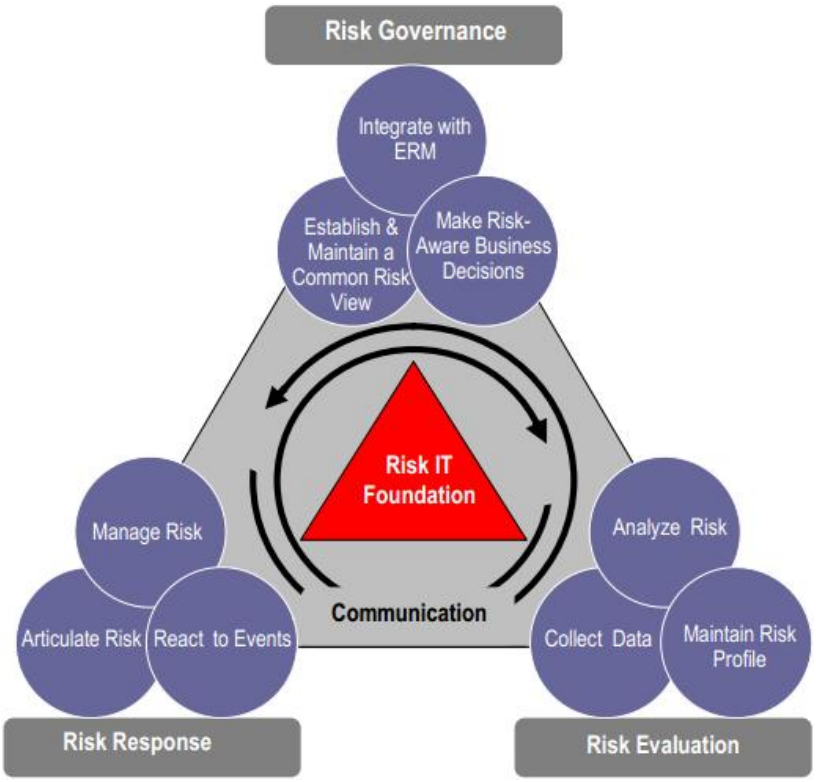
Figura 17: Principios de los riesgos de TI

Fuente: (ISACA, 2009)

2.2.5.5. PROCESO INTEGRAL MARCO DE TRABAJO RISK IT

El marco de los riesgos de TI se basa en los principios establecidos en el punto anterior, y se ha desarrollado en base a un modelo de proceso integral. El modelo del proceso en la gestión de riesgos fija ciertas actividades clave en una serie de procesos, estos procesos se agrupan en tres ámbitos: Gobierno del riesgo, Evaluación del Riesgo y Respuesta ante el Riesgos; cada uno de los cuales contiene tres procesos, tal y como se muestra en la Figura 18.

Figura 18: Marco del riesgo de TI



Fuente: (ISACA, 2009)

2.2.5.6. FUNDAMENTOS DEL GOBIERNO DE RIESGOS DE TI

Este proceso trata sobre algunos de los componentes esenciales del dominio de Gobierno del Riesgo. Los temas tratados incluyen:

- El apetito del riesgo y la tolerancia al riesgo.
- Responsabilidades y rendición de cuentas sobre la gestión de riesgos de TI.
- Sensibilización y comunicación.
- Cultura del riesgo.

2.2.5.7. FUNDAMENTOS DE LA EVALUACIÓN DE RIESGOS

A continuación se describen los sub procesos que son parte del proceso de evaluación de riesgos:

- Descripción del impacto de la organización:

  La evaluación significativa de riesgos de TI y el riesgo - de decisiones basadas en los riesgos de TI requieren ser expresadas en términos inequívocos y claros relevantes de negocios. La gestión efectiva del riesgo requiere de la comprensión mutua entre TI y el negocio sobre el que el riesgo debe ser gestionado y por qué. Todas las partes interesadas deben tener la capacidad de comprender y expresar cómo los eventos adversos pueden afectar a los objetivos de negocio. Esto significa que una persona de TI debe comprender como los fallos relacionados o acontecimientos relacionados con TI pueden afectar a los objetivos de la organización y causar perdida directa o indirecta a la organización y también significa que una persona del negocio debe entender cómo los fallos o eventos relacionados con TI pueden afectar a los servicios y procesos clave.

  El vínculo entre la TI y el impacto de escenarios de riesgo organizacional fundamental debe ser establecido para comprender los efectos de los eventos adversos. Varias técnicas y opciones existen que pueden ayudar a la organización para describirlo en términos de riesgos de negocios. El marco de riesgos de TI requiere riesgos para la traducir o expresado en términos pertinentes con la organización, pero no prescribe

ningún método único. Algunos métodos disponibles se muestran en la Figura 19 y se discuten brevemente en lo que resta de esta sección. Para más detalles sobre los métodos descritos en la Figura 19 y orientación sobre cómo aplicarlas en la práctica se incluyen en la Guía Profesional de riesgos de TI.

Figura 19: Expresando riesgos de TI en términos de negocio

Fuente: (ISACA, 2009)

- Escenarios de riesgos de TI

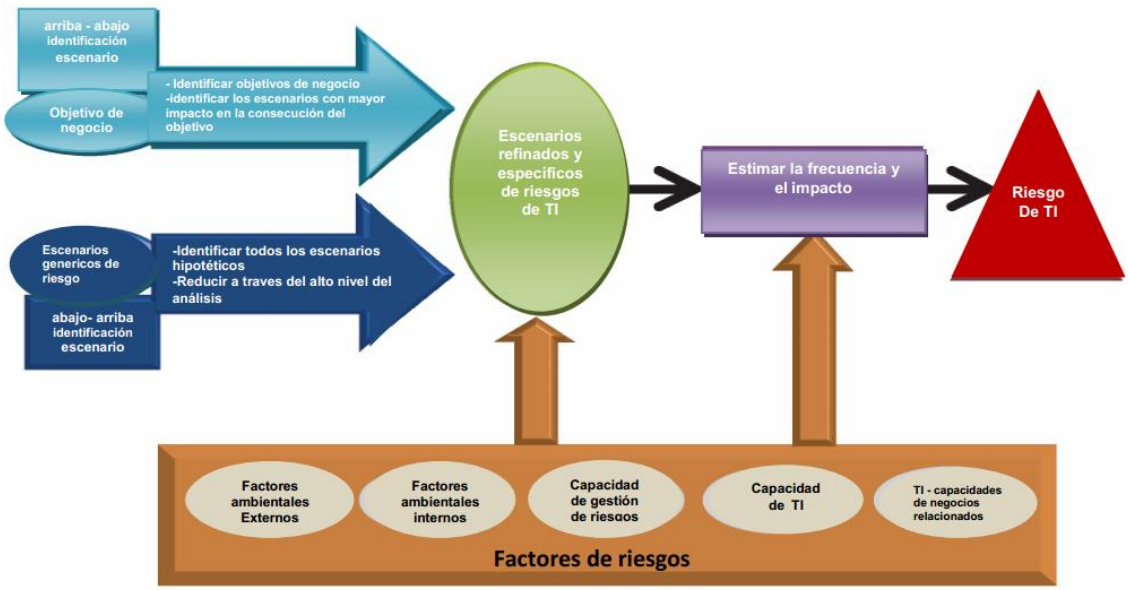
Uno de los desafíos para la gestión de riesgos de TI debe identificar los riesgos importantes y relevantes entre todo lo que posiblemente puede relacionarse con TI, considerando la presencia y dependencia de TI en el negocio. Una de las técnicas para vencer este desafío es el desarrollo y el empleo de argumentos de riesgo, el cual es un enfoque básico para lograr el realismo, visión, compromiso organizacional, mejorar el análisis y la estructura de la compleja cuestión de los riesgos de TI.

Una vez que se desarrollan estos escenarios, estos se utilizan durante el análisis de riesgo, donde la frecuencia de la situación realmente está sucediendo y los impactos comerciales son estimaciones.

La Figura 20 muestra que los escenarios de riesgo se pueden derivar a través de dos mecanismos diferentes: Un enfoque de arriba - abajo y un enfoque de abajo - arriba.

Los enfoques son complementarios y deben ser utilizados simultáneamente. De hecho, los escenarios de riesgo deben ser pertinentes y deben estar vinculados con el riesgo real de negocio. Por otra parte, utilizar un conjunto de escenarios de riesgo genérico ayuda a asegurar que no se pasan por alto los riesgos y proporciona una visión más amplia y completa sobre los riesgos de TI. Una vez que el conjunto de escenarios de riesgo se define, puede ser utilizado para el análisis de riesgos, donde se evalúa la frecuencia y el impacto del escenario. Un componente importante de esta evaluación son los factores de riesgo, tal como se muestra en la Figura 20.

Figura 20: Desarrollo de escenarios de riesgo de TI

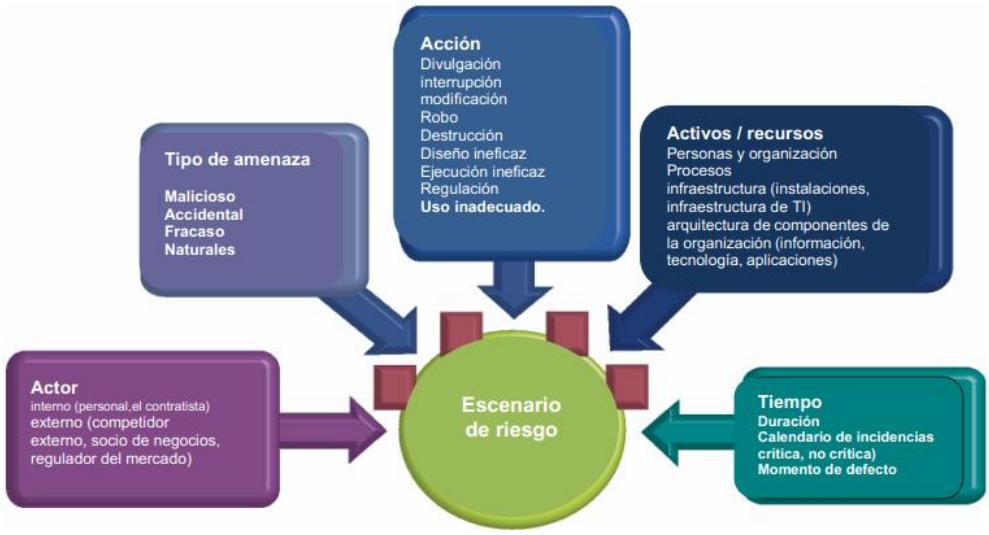


Fuente: (ISACA, 2009)

Un escenario de riesgo es la descripción de un evento relacionado con TI que puede conducir a un impacto en el negocio. Para que los escenarios de riesgos sean

completos y se puedan utilizar en análisis de riesgos, deben contener algunos componentes, que se muestran en la Figura 21.

Figura 21: Componentes de escenario de riesgo



Fuente: (ISACA, 2009)

2.2.5.8. FUNDAMENTOS DE LA RESPUESTA DE RIESGOS

Principalmente debe definirse y priorizarse las respuestas a los riesgos, para llevar el riesgo al mismo nivel definido en el apetito de riesgo de la empresa. En otras palabras, las respuestas a los riesgos deben ser definidas de tal manera que dichos riesgos no representen una potencial pérdida para la organización, para lo cual se tienen distintos tipos de respuesta:

- Evitar riesgos:

  Evitar significa salir de las actividades o de las condiciones que dan lugar a un riesgo, el mismo se aplica cuando no hay otra respuesta adecuada. Este es el caso cuando no hay ninguna otra respuesta rentable que puede tener éxito en la reducción de la frecuencia y de la magnitud por debajo de los umbrales definidos para el apetito del

riesgo, o cuando el riesgo no puede ser compartido o transferido y también si el riesgo se juzga inaceptable por la administración.

Algunos ejemplos relacionados con la cobertura de riesgos de TI pueden incluir la reubicación de un centro de datos fuera de una región con importantes peligros naturales, o negarse a participar en un proyecto muy grande, cuando el caso de negocio muestra un notable riesgo de fracaso.

- Reducción de riesgos:

  La reducción significa qué medidas están tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto de un riesgo. Las maneras más comunes de respuesta al riesgo incluyen el fortalecimiento global de la gestión de las prácticas de riesgos de TI, es decir, aplicación de la suficiente madurez de la gestión de riesgos y los procesos que deben definirse como el marco de riesgos de TI y también la introducción de una serie de medidas de control intentando reducir las frecuencias de un suceso de consecuencias adversas y/o el impacto empresarial de un evento, en caso de que suceda.

- Riesgo compartido:

  Compartir significa reducir la frecuencia de riesgo o impacto mediante la transferencia o distribución de una parte del riesgo. Las técnicas más comunes son los seguros y la subcontratación.

  Los ejemplos incluyen tener un seguro para los incidentes relacionados con las TI, la subcontratación de parte de las actividades de TI, o establecer un proyecto de riesgo de TI compartido con el proveedor a través de acuerdos de precios fijos o acuerdos de

inversión compartida. Tanto en un sentido físico y jurídico estas técnicas no alivian una empresa de un riesgo, pero puede afectar la capacidad de la otra parte en la gestión del riesgo y reducir las consecuencias económicas si se produce un evento adverso.

- Aceptación del riesgo:

  Aceptación significa que no se tomen medidas relativas con un riesgo particular, y la pérdida es aceptada cuando y si se produce. Esto es diferente de ignorar el riesgo, aceptar el riesgo supone que el riesgo es conocido, es decir, una decisión informada se ha aceptado por la dirección. Si una empresa adopta una postura de aceptación de riesgo, se debe considerar cuidadosamente quién puede asumir el riesgo, más aún con los riesgos de TI.

  Los riesgos de TI deben ser aceptados por la dirección de la empresa (y los propietarios de procesos de negocio) con la colaboración y el apoyo de TI, y la aceptación debe ser comunicada a la Junta. Si un riesgo particular es evaluado por ser extremadamente raro, pero muy importante (catastrófico) y los enfoques para reducirla son prohibitivos, la administración puede decidir aceptarlo.

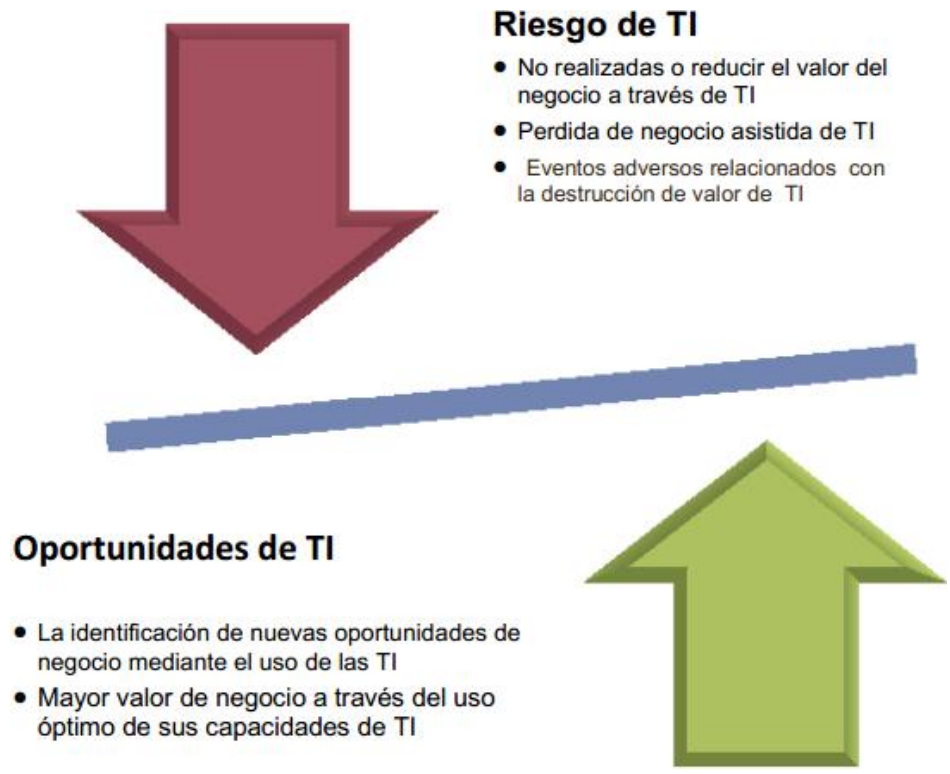
2.2.5.9. RIESGOS Y OPORTUNIDADES DE GESTIÓN USANDO COBIT, VAL IT Y RISK IT

En un día típico en una organización típica, las actividades de TI, los procesos de TI están organizados y desplegados. Se producen eventos en varias áreas: las opciones tecnológicas deben ser evaluadas, las reparaciones en caso de incidentes operacionales deben ser aplicadas, los problemas de software deben ser abordados y las solicitudes deben ser respondidas. Cada uno de estos eventos lleva un cierto riesgo y oportunidad.

El riesgo refleja la combinación de la frecuencia de los hechos ocurridos y el impacto que tienen estos acontecimientos sobre la organización. El riesgo potencial para los acontecimientos y sus consecuencias contiene las oportunidades de beneficio (al revés) o de amenazas para el éxito (negativo). Riesgo y oportunidad van juntas, de hecho, para proporcionar valor de negocio a los interesados, las empresas deben participar en diversas actividades e iniciativas (oportunidades), todos conllevan grado de incertidumbre y, por tanto, de riesgo.

La gestión del riesgo y de la oportunidad es una actividad estratégica clave para el éxito de la organización. TI pueden jugar varios roles en relación riesgo-oportunidad, tal cual se muestra en la Figura 22.

Figura 22: Riesgo y oportunidad



Fuente: (ISACA, 2009)

2.3. GLOSARIO DE TÉRMINOS BÁSICOS

2.3.1. AMENAZA

Según el diccionario (Real Academia Española, 2017), es dar a entender con actos o palabras que se quiere hacer algún mal a alguien.

2.3.2. APETITO POR EL RIESGO

Es la cantidad de riesgo que una organización está dispuesta a aceptar en el cumplimiento de su misión o visión. Este depende de la capacidad objetiva de la organización para absorber pérdidas y, la cultura o predisposición a asumir riesgos prudentes o agresivos para alcanzar sus objetivos estratégicos. (Superintendencia de Banca y Seguros, 2009)

2.3.3. CONTROL INTERNO

Es un proceso, realizado por el Directorio, la Gerencia y el personal, diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones. (Superintendencia de Banca y Seguros, Resolución SBS N° 37-2008, 2008)

2.3.4. EVENTO

Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo. (Superintendencia de Banca y Seguros, Resolución SBS N° 37-2008, 2008)

2.3.5. GESTIÓN DE RIESGOS

Consiste en el método para determinar, analizar, valorar y clasificar el riesgo al cual se encuentra expuesta una organización, con el fin de implementar mecanismos que permitan

controlar y mantener los riesgos en un nivel tolerable. La gestión de riesgos se encuentra formada por cuatro fases: Análisis, clasificación, reducción y control de riesgos. (ISO 31000:2009, 2009)

2.3.6. GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

Relacionado al manejo de las fallas de seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos. (Superintendencia de Banca y Seguros, 2009)

2.3.7. IMPACTO

Es la consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. También es llamado severidad. (Superintendencia de Banca y Seguros, Resolución SBS N° 37-2008, 2008)

2.3.8. MARCO DE TRABAJO RISK IT

Conjunto estandarizado de buenas prácticas para identificar, gobernar y administrar los riesgos de tecnología asociados al negocio de las organizaciones. (ISACA, 2009)

2.3.9. NIVEL DE RIESGO

Se obtiene a partir de la combinación del impacto y la probabilidad, ésta indica el grado de severidad que podría tener un determinado riesgo. (Superintendencia de Banca y Seguros, Resolución SBS N° 37-2008, 2008)

2.3.10. PROBABILIDAD

La posibilidad de la ocurrencia de un evento que usualmente es aproximada mediante una distribución estadística. En ausencia de información suficiente, o donde no resulta posible obtenerla, se puede aproximar mediante métodos cualitativos. (Superintendencia de Banca y Seguros, Resolución SBS N° 37-2008, 2008)

2.3.11. RIESGO

Según el Diccionario (Real Academia Española, 2017), la palabra riesgo viene del árabe rizq (lo que depara la providencia) a través del italiano rischio. Riesgo, se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas; el riesgo se encuentra vinculado a la vulnerabilidad y amenaza.

2.3.12. SEGURIDAD DE LA INFORMACIÓN

Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad. (Hildago Nuchera, 2014)

2.3.13. TECNOLOGÍA DE INFORMACIÓN

La tecnología de la información (TI, o más conocida como IT por su significado en inglés: information technology) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas. (Roig, 2015)

2.3.14. TOLERANCIA AL RIESGO

Es el nivel de variación que la empresa está dispuesta a asumir en caso de desviación a los objetivos empresariales trazados. (Superintendencia de Banca y Seguros, 2009)

2.3.15. VULNERABILIDAD

Condiciones, características y capacidad de un sistema que lo hacen susceptible a amenazas y, como resultado se ven expuestas a sufrir algún daño. Corresponde a los acontecimientos que contribuyen a la magnitud o frecuencia de eventos de pérdida que ocurren. (Ernst & Young, 2012)

2.4. HIPÓTESIS DE LA INVESTIGACIÓN

2.4.1. HIPÓTESIS GENERAL

La presente investigación al ser de tipo descriptiva no tiene hipótesis.

2.5. OPERACIONALIZACIÓN DE VARIABLES

La operacionalización de variables utilizada para la presente investigación se muestra en el Cuadro 1.

Cuadro 1: Operación de Variables

Variable	Indicadores	Dimensiones	Técnicas	Instrumentos
Variable Dependiente: Gestión de Riesgos de Tecnología de Información	Gobierno del Riesgo.	- Visión común de riesgo. - Integración con el ERM. - Conciencia de los riesgos del negocio.	- Encuesta. - Observación.	- Modelo de Madurez del Gobierno de Riesgo. - Guía de Observación.
	Evaluación de Riesgos.	- Recolección de datos. - Análisis de riesgos de TI. - Mantenimiento del perfil de riesgo.	- Encuesta. - Observación.	- Modelo de Madurez de la Evaluación de Riesgos. - Guía de Observación.
	Respuesta a los Riesgos.	- Articulación del riesgo. - Gestión del riesgo. - Reacción a los eventos.	- Encuesta. - Observación.	- Modelo de Madurez de Respuesta a los Riesgos. - Guía de Observación.

Elaboración: Propia

CAPÍTULO III

DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

3.1. TIPO Y DISEÑO DE LA INVESTIGACIÓN

De acuerdo con las características del problema y los objetivos, la presente investigación tuvo un enfoque cualitativo y por lo tanto el tipo de investigación fue no experimental.

Asimismo, el diseño de la investigación fue descriptiva, puesto que la presente tesis pretendía describir el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes S.A. en el periodo Diciembre 2014 a Diciembre 2015.

3.2. POBLACIÓN Y MUESTRA DE INVESTIGACIÓN

3.2.1. POBLACIÓN

Los procesos de la Gestión de Riesgos de Tecnologías de Información son soportados principalmente por la Gerencia de Tecnologías de Información de la Caja Rural de Ahorro y Créditos “Los Andes” S.A., asimismo todos sus trabajadores al usar productos y servicios que esta brinda también son partícipes de la gestión de riesgos mencionada, por lo cual el tamaño de la población se ha determinado en el Cuadro 2.

Cuadro 2: Población de la Investigación

Categoría Laboral	Cantidad de Población
Gerentes	2
Funcionarios	36
Empleados	470
Otros	14
TOTAL	**522**

Elaboración: Propia

El tamaño total de la población de acuerdo al cuadro anterior fue de 522 personas que laboraban en la Caja Rural de Ahorro y Créditos "Los Andes" S.A. durante el periodo 2015.

3.2.2. MUESTRA

El tipo de muestra de la presente investigación fue no probabilístico intencional porque las unidades fueron determinadas de acuerdo a la experiencia del investigador en función a los propósitos de la investigación (Mitacc Meza, 2011).

Asimismo, con el propósito de describir el nivel de madurez de la Gestión de Riesgos de Tecnología de Información se realizaron dos encuestas, una para el periodo Diciembre 2014 y otra para el periodo Diciembre 2015, cada encuesta fue completada en base a la observación del investigador y en base a la intervención de todos los involucrados en los procesos de Tecnología de Información de la Caja Rural de Ahorro y Crédito "Los Andes" S.A.

3.3. UBICACIÓN Y DESCRIPCIÓN DE LA POBLACIÓN

PAÍS: Perú

DEPARTAMENTO: Puno

PROVINCIA: Puno

DISTRITO: Puno

LUGAR: Caja Rural de Ahorro y Crédito "Los Andes" S.A.

3.4. TÉCNICAS E INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN

Las técnicas que se utilizaron en el presente proyecto de investigación fueron las que se describen a continuación:

3.4.1. TÉCNICAS

- **ENCUESTA:** Según Arias (2006) Es una técnica que pretende obtener información que suministra un grupo o muestra de sujetos acerca de si mismos, o en relación con un tema en particular." (Pág. 72). Esta técnica permitió la recolección de información directamente del personal que participa en los procesos de Gestión de Riesgos de Tecnología de Información de la Caja Rural de Ahorro y Crédito "Los Andes" S.A.
- **OBSERVACIÓN:** Es una técnica que permitió tener contacto directo con la realidad y con quienes se hicieron las entrevistas, lo cual ayudó a obtener un mayor conocimiento de la realidad de la Gestión de Riesgos de Tecnología de Información.

3.4.2. INSTRUMENTOS

- **MODELO DE MADUREZ:** Este instrumento ha sido utilizado para determinar el nivel de madurez de la Gestión de Riesgos de Tecnología de Información, dicho modelo

consta de 209 preguntas, de los cuales 100 corresponden al indicador de "Gobierno del Riesgo", 55 corresponden al indicador de "Evaluación del Riesgo" y 54 corresponden al indicador de "Respuesta al Riesgo".

- **GUÍA DE OBSERVACIÓN:** Este instrumento se utilizó para establecer el contexto de observación durante la presente investigación.

3.5. TÉCNICAS PARA EL PROCESAMIENTO Y ANÁLISIS DE DATOS

Las técnicas que se utilizaron en el presente proyecto de investigación para el procesamiento y análisis de datos son las siguientes:

- Ordenamiento y codificación de datos.
- Tabulación de datos.
- Tablas estadísticas.
- Gráficos estadísticos.
- Análisis e interpretación de datos.

3.6. PLAN DE TRATAMIENTO DE LOS DATOS

Los datos fueron tratados y analizados en su totalidad con hojas de cálculo de Excel para que se tenga más orden en el procesamiento de la información recolectada.

Una vez recolectados los datos mediante las técnicas e instrumentos establecidos, se procesó la información en hojas de Excel de Microsoft Office y se obtuvo el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información. Posteriormente, se analizaron los resultados, se interpretaron a través de gráficos y finalmente estos fueron descritos.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

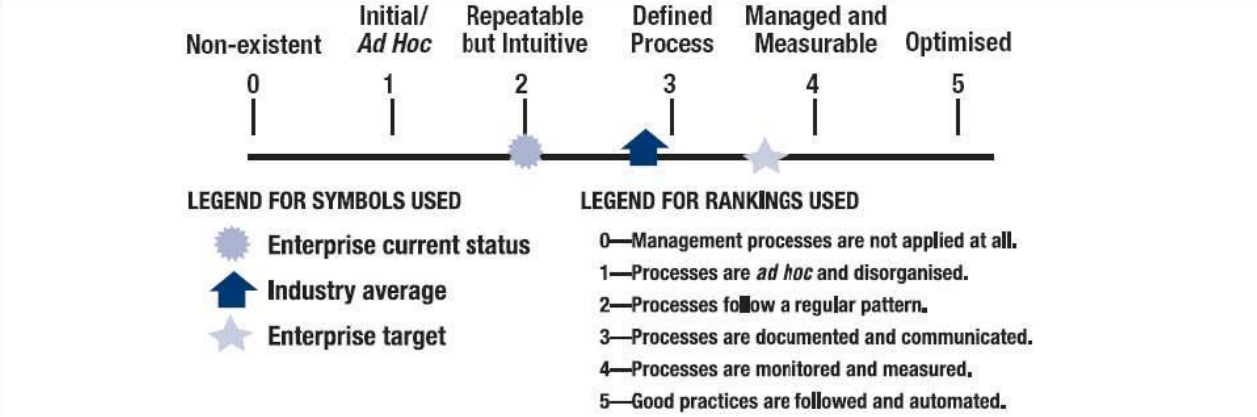
El objetivo de la presente investigación es describir el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito "Los Andes" S.A. en el periodo Diciembre 2014 a Diciembre 2015, por ello, en este apartado se han analizado y procesado los datos recogidos de las encuestas del Modelo de Madurez de la Gestión de Riesgos de Tecnología de Información.

La metodología seguida constó de dos partes. La primera, "Describir el nivel de madurez de la Gestión de Riesgos de Tecnología de Información en el periodo Diciembre 2014". La segunda parte, "Describir el nivel de madurez de la Gestión de Riesgos de Tecnología de Información en el periodo Diciembre 2015".

4.1. CARACTERÍSTICAS DE LA ENCUESTA DEL MODELO DE MADUREZ

El modelo de madurez de la Gestión de Riesgos de Tecnología de Información permite determinar qué tan preparada se encuentra la empresa para gestionar los riesgos tecnológicos a los cuales se encuentra expuesta. La Figura 23, muestra los niveles de madurez definidos.

Figura 23: Modelo de Madurez



Fuente: (ISACA, 2009)

A continuación se describen todos los niveles establecidos en el Modelo de Madurez:

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

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

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

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

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

En el nivel 1, se cuenta con controles implementados, enfocados al cumplimiento de requisitos del negocio que han sido aplicados de forma aislada lo cual puede ocasionar que áreas diferentes controlen sus riesgos de forma independiente.

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

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

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

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

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

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

  El nivel 3 requiere que los procesos se definan claramente planteando el propósito, entradas, criterios de entrada, actividades, roles, medidas, pasos de verificación, salidas

y criterios de salida, asimismo que sean manejados proactivamente entendiendo las interrelaciones de las actividades y medidas detalladas del proceso, sus artefactos y sus servicios.

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

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

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

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

cuantitativos se definen en base a necesidades del cliente, usuarios finales, organización y actores de los procesos.

En este nivel existe un crecimiento, mejora y redefinición que permite actualizar continuamente la gestión del riesgo que incluye la forma de articular el riesgo, mitigación, reacción ante la materialización del mismo y aprovechamiento de las oportunidades que conlleva la mitigación; para esto se utilizan los controles para establecer causas comunes de variación en los procesos y así modificar los procesos para alcanzar mejores resultados. Se utilizan herramientas para gestionar el riesgo de cartera del negocio, supervisar los controles, recursos y capacidades de la empresa.

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

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

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

La encuesta del modelo de madurez se basa en los tres dominios que cubre el Marco de Trabajo RISK IT la cual contiene una serie de preguntas puntuales que permiten establecer la frecuencia con la cual se realizan ciertas actividades relacionadas a la Gestión de Riesgos de Tecnología de Información.

Esta investigación se centró solamente en describir el nivel de madurez de la Caja Rural de Ahorro y Crédito “Los Andes” S.A. para gestionar el riesgo no incluyendo la identificación de riesgos puntuales ni el nivel de exposición a cada uno de estos.

La recopilación de datos se dio mediante entrevistas a los principales roles de la organización relacionados a la Gestión de TI y la Gestión de Riesgos de TI, asimismo a través de la observación y la experiencia del investigador.

Para describir la frecuencia con que se realizan las actividades relacionadas a la Gestión de Riesgos de TI, se trabajó con una escala de 6 niveles los cuales se citan en el Cuadro 3.

Cuadro 3: Escalas de Evaluación

Valor	Descripción	Nivel de Madurez	Frecuencia
0	Los procesos de manejo de riesgos no son aplicados.	No Existe	Nunca
1	Los procesos son Ad Hoc y desorganizados.	Inicial	Rara Vez
2	Los procesos siguen un patrón regular.	Repetible	A Veces
3	Los procesos son documentados y comunicados.	Definido	Frecuentemente
4	Los procesos son supervisados y medidos.	Gestionado	Casi Siempre
5	Las mejores prácticas son seguidas y automatizadas.	Optimizado	Siempre

Elaboración: Propia

Para describir el estado general y el nivel de madurez de la Gestión de Riesgos de TI, se plantearon una serie de preguntas que representan aspectos fundamentales a cubrir para la Gestión de Riesgos, los cuales se agruparon en las categorías mostradas a continuación:

4.1.1. INDICADORES

Los dominios del Marco de Trabajo RISK IT son los mismos que los indicadores definidos para la presente investigación, por lo tanto se evaluó la aplicación de dichos dominios clasificándolos según las categorías definidas en el Cuadro 4.

Cuadro 4: Dominios del Marco de Trabajo RISK IT

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

Elaboración: Propia

4.1.2. PROCESOS DEL MARCO DE TRABAJO RISK IT

Alineado al Marco de Trabajo RISK IT, se evaluó también la aplicación de los nueve procesos definidos en el marco clasificándolos según las categorías definidas en el Cuadro 5.

Cuadro 5: Procesos del Marco de Trabajo RISK IT

ID	Proceso	Descripción
RG1	Establecer y mantener una visión común del riesgo.	Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la empresa de TI relacionados con la pérdida de liderazgo y la tolerancia subjetiva de ella.
RG2	Integrar con la Gestión de Riesgos Empresariales.	Integrar la estrategia y las operaciones de gestión de riesgos de TI con las decisiones estratégicas de riesgo de negocio que se han tomado a nivel de empresa.
RG3	Tomar decisiones del negocio con conciencia del riesgo.	Asegurar que las decisiones de la organización toman en cuenta la amplia gama de oportunidades y consecuencias generadas de la dependencia de la TI, para el éxito.
RE1	Recopilar datos.	Identificar los datos pertinentes para hacer viable la identificación de riesgos de TI, el análisis y presentación de informes.
RE2	Analizar el riesgo.	Desarrollar información útil para apoyar las decisiones de riesgo, que tenga en cuenta la importancia de factores de riesgo de negocios.
RE3	Mantener el perfil de riesgo.	Mantener actualizado el inventario completo de los riesgos conocidos y los atributos (por ejemplo, que se espera, la frecuencia de impacto potencial, disposición), los recursos, las capacidades y los controles como se entiende en el contexto de los productos empresariales, servicios y procesos.

Continúa…

RR1	Articular el riesgo.	Garantizar que la información sobre el estado real de las exposiciones y las oportunidades relacionadas con TI se pone a disposición en forma oportuna y a las personas adecuadas para una respuesta adecuada.
RR2	Gestionar el riesgo.	Garantizar que las medidas para aprovechar las oportunidades estratégicas y reducir los riesgos a un nivel aceptable se gestionan como un portafolio.
RR3	Reaccionar ante eventos.	Asegurar que las medidas para aprovechar las oportunidades inmediatas o limitar la magnitud de la pérdida de los acontecimientos relacionados con la TI se activan de forma oportuna y eficaz.

Elaboración: Propia

4.1.3. ACTIVIDADES DEL MARCO DE TRABAJO RISK IT

Las categorías definidas agruparon una serie de interrogantes que conforman la encuesta de evaluación del nivel de madurez de la Gestión de Riesgos de TI, las cuales buscaron describir el nivel de cumplimiento de las actividades de gestión de riesgos de TI definidos en el Marco de Trabajo de RISK IT, las mismas que se listan en el Cuadro 6.

Cuadro 6: Actividades del Marco de Trabajo RISK IT

ID	Actividad	ID Proceso	ID Dominio
RG1.1	Realizar evaluación de riesgos de TI en toda la organización.	RG1	RG

Continúa…

RG1.2	Proponer límites de tolerancia al riesgo de TI.	RG1	RG
RG1.3	Aprobar la tolerancia al riesgo de TI.	RG1	RG
RG1.4	Alinear la política del riesgo de TI.	RG1	RG
RG1.5	Promover la cultura consciente de los riesgos de TI.	RG1	RG
RG1.6	Fomentar la comunicación efectiva del riesgo de TI.	RG1	RG
RG2.1	Establecer y mantener responsabilidades para la gestión de riesgos de TI.	RG2	RG
RG2.2	Coordinar la estrategia del riesgo de TI y la estrategia del riesgo del negocio.	RG2	RG
RG2.3	Adaptar las prácticas del riesgo de TI a las prácticas del riesgo empresarial.	RG2	RG
RG2.4	Proporcionar los recursos adecuados para la gestión del riesgo de TI.	RG2	RG
RG2.5	Proporcionar aseguramiento independiente sobre la gestión del riesgo de TI.	RG2	RG
RG3.1	Adquirir la aceptación de la gerencia para el enfoque del análisis de riesgos de TI.	RG3	RG
RG3.2	Aprobar el análisis de riesgos de TI.	RG3	RG

Continúa…

RG3.3	Incorporar las consideraciones del riesgo de TI en la toma de decisiones estratégicas del negocio.	RG3	RG
RG3.4	Aceptar el riesgo de TI.	RG3	RG
RG3.5	Priorizar las actividades de respuesta a los riesgos de TI.	RG3	RG
RE1.1	Establecer y mantener un modelo para recopilar datos.	RE1	RE
RE1.2	Recopilar datos sobre el entorno operativo.	RE1	RE
RE1.3	Recopilar datos sobre eventos de riesgo.	RE1	RE
RE1.4	Identificar factores de riesgo.	RE1	RE
RE2.1	Definir el alcance del análisis del riesgo de TI.	RE2	RE
RE2.2	Estimar el riesgo de TI.	RE2	RE
RE2.3	Identificar las opciones de respuesta al riesgo.	RE2	RE
RE2.4	Realizar una revisión por pares del análisis de riesgos de TI.	RE2	RE
RE3.1	Mapear los recursos de TI para los procesos del negocio.	RE3	RE
RE3.2	Determinar la criticidad de los recursos de TI para el negocio.	RE3	RE
RE3.3	Comprender las capacidades de TI.	RE3	RE
RE3.4	Actualizar los componentes del escenario del riesgo de TI.	RE3	RE
RE3.5	Mantener el registro de los riesgos de TI y el mapa de riesgos de TI.	RE3	RE

Continúa…

RE3.6	Desarrollar indicadores de riesgos de TI.	RE3	RE
RR1.1	Comunicar los resultados del análisis del riesgo de TI.	RR1	RR
RR1.2	Informar las actividades de la gestión de riesgos de TI y el estado de cumplimiento.	RR1	RR
RR1.3	Interpretar resultados de evaluaciones independientes del riesgo de TI.	RR1	RR
RR1.4	Identificar las oportunidades relacionadas con TI.	RR1	RR
RR2.1	Inventario de controles.	RR2	RR
RR2.2	Monitorear la alineación operacional con los umbrales de tolerancia al riesgo.	RR2	RR
RR2.3	Responder a la exposición y oportunidad de los riesgos identificados.	RR2	RR
RR2.4	Implementar controles.	RR2	RR
RR2.5	Informar el progreso del plan de acción de los riesgos de TI.	RR2	RR
RR3.1	Mantener planes de respuesta a incidentes.	RR3	RR
RR3.2	Monitorear el riesgo de TI.	RR3	RR
RR3.3	Iniciar respuesta a incidente.	RR3	RR
RR3.4	Comunicar las lecciones aprendidas de los eventos de riesgo.	RR3	RR

Elaboración: Propia

Por otro lado, la encuesta del modelo de madurez se compuso por 209 preguntas relacionadas a los 3 dominios, 9 procesos y 43 actividades del Marco de Trabajo RISK IT, los mismos que se distribuyeron de acuerdo a los Cuadros 7, 8 y 9.

Cuadro 7: Cantidad de Preguntas por Indicador

ID	Indicador (Dominio)	Listado de Preguntas	Total de Preguntas
RG	Gobierno del Riesgo.	Del 1 al 100	100
RE	Evaluación del Riesgo.	Del 101 al 155	55
RR	Respuesta al Riesgo.	Del 156 al 209	54

Elaboración: Propia

Cuadro 8: Cantidad de Preguntas por Proceso

ID	Proceso	Listado de Preguntas	Total de Preguntas
RG1	Establecer y mantener una visión común del riesgo.	Del 1 al 45	45
RG2	Integrar con la Gestión de Riesgos Empresariales.	Del 46 al 77	32
RG3	Tomar decisiones del negocio con conciencia del riesgo.	Del 78 al 100	23
RE1	Recopilar datos.	Del 101 al 114	14
RE2	Analizar el riesgo.	Del 115 al 131	17
RE3	Mantener el perfil de riesgo.	Del 132 al 155	24

Continúa…

RR1	Articular el riesgo.	Del 156 al 171	16
RR2	Gestionar el riesgo.	Del 172 al 192	21
RR3	Reaccionar ante eventos.	Del 193 al 209	17

Elaboración: Propia

Cuadro 9: Cantidad de Preguntas por Actividad

ID	Actividad	Listado de Preguntas	Total de Preguntas
RG1.1	Realizar evaluación de riesgos de TI en toda la organización.	Del 1 al 12	12
RG1.2	Proponer límites de tolerancia al riesgo de TI.	Del 13 al 16	4
RG1.3	Aprobar la tolerancia al riesgo de TI.	Del 17 al 22	6
RG1.4	Alinear la política del riesgo de TI.	Del 23 al 30	8
RG1.5	Promover la cultura consciente de los riesgos de TI.	Del 31 al 37	7
RG1.6	Fomentar la comunicación efectiva del riesgo de TI.	Del 38 al 45	8
RG2.1	Establecer y mantener responsabilidades para la gestión de riesgos de TI.	Del 46 al 56	11
RG2.2	Coordinar la estrategia del riesgo de TI y la estrategia del riesgo del negocio.	Del 57 al 67	11

Continúa…

RG2.3	Adaptar las prácticas del riesgo de TI a las prácticas del riesgo empresarial.	Del 68 al 73	6
RG2.4	Proporcionar los recursos adecuados para la gestión del riesgo de TI.	Del 74 al 76	3
RG2.5	Proporcionar aseguramiento independiente sobre la gestión del riesgo de TI.	Del 77 al 77	1
RG3.1	Adquirir la aceptación de la gerencia para el enfoque del análisis de riesgos de TI.	Del 78 al 81	4
RG3.2	Aprobar el análisis de riesgos de TI.	Del 82 al 84	3
RG3.3	Incorporar las consideraciones del riesgo de TI en la toma de decisiones estratégicas del negocio.	Del 85 al 89	5
RG3.4	Aceptar el riesgo de TI.	Del 90 al 95	6
RG3.5	Priorizar las actividades de respuesta a los riesgos de TI.	Del 96 al 100	5
RE1.1	Establecer y mantener un modelo para recopilar datos.	Del 101 al 104	4
RE1.2	Recopilar datos sobre el entorno operativo.	Del 105 al 108	4
RE1.3	Recopilar datos sobre eventos de riesgo.	Del 109 al 110	2
RE1.4	Identificar factores de riesgo.	Del 111 al 114	4
RE2.1	Definir el alcance del análisis del riesgo de TI.	Del 115 al 117	3
RE2.2	Estimar el riesgo de TI.	Del 118 al 123	6

Continúa…

RE2.3	Identificar las opciones de respuesta al riesgo.	Del 124 al 127	4
RE2.4	Realizar una revisión por pares del análisis de riesgos de TI.	Del 128 al 131	4
RE3.1	Mapear los recursos de TI para los procesos del negocio.	Del 132 al 134	3
RE3.2	Determinar la criticidad de los recursos de TI para el negocio.	Del 135 al 137	3
RE3.3	Comprender las capacidades de TI.	Del 138 al 140	3
RE3.4	Actualizar los componentes del escenario del riesgo de TI.	Del 141 al 145	5
RE3.5	Mantener el registro de los riesgos de TI y el mapa de riesgos de TI.	Del 146 al 150	5
RE3.6	Desarrollar indicadores de riesgos de TI.	Del 151 al 155	5
RR1.1	Comunicar los resultados del análisis del riesgo de TI.	Del 156 al 160	5
RR1.2	Informar las actividades de la gestión de riesgos de TI y el estado de cumplimiento.	Del 161 al 163	3
RR1.3	Interpretar resultados de evaluaciones independientes del riesgo de TI.	Del 164 al 168	5
RR1.4	Identificar las oportunidades relacionadas con TI.	Del 169 al 171	3
RR2.1	Inventario de controles.	Del 172 al 176	5

Continúa…

RR2.2	Monitorear la alineación operacional con los umbrales de tolerancia al riesgo.	Del 177 al 181	5
RR2.3	Responder a la exposición y oportunidad de los riesgos identificados.	Del 182 al 185	4
RR2.4	Implementar controles.	Del 186 al 190	5
RR2.5	Informar el progreso del plan de acción de los riesgos de TI.	Del 191 al 192	2
RR3.1	Mantener planes de respuesta a incidentes.	Del 193 al 197	5
RR3.2	Monitorear el riesgo de TI.	Del 198 al 201	4
RR3.3	Iniciar respuesta a incidente.	Del 202 al 204	3
RR3.4	Comunicar las lecciones aprendidas de los eventos de riesgo.	Del 205 al 209	5

Elaboración: Propia

La encuesta del Modelo de Madurez utilizada para los periodos Diciembre 2014 y Diciembre 2015 se encuentra en el Anexo 1 del presente documento.

4.2. RESULTADOS DE LA INVESTIGACIÓN

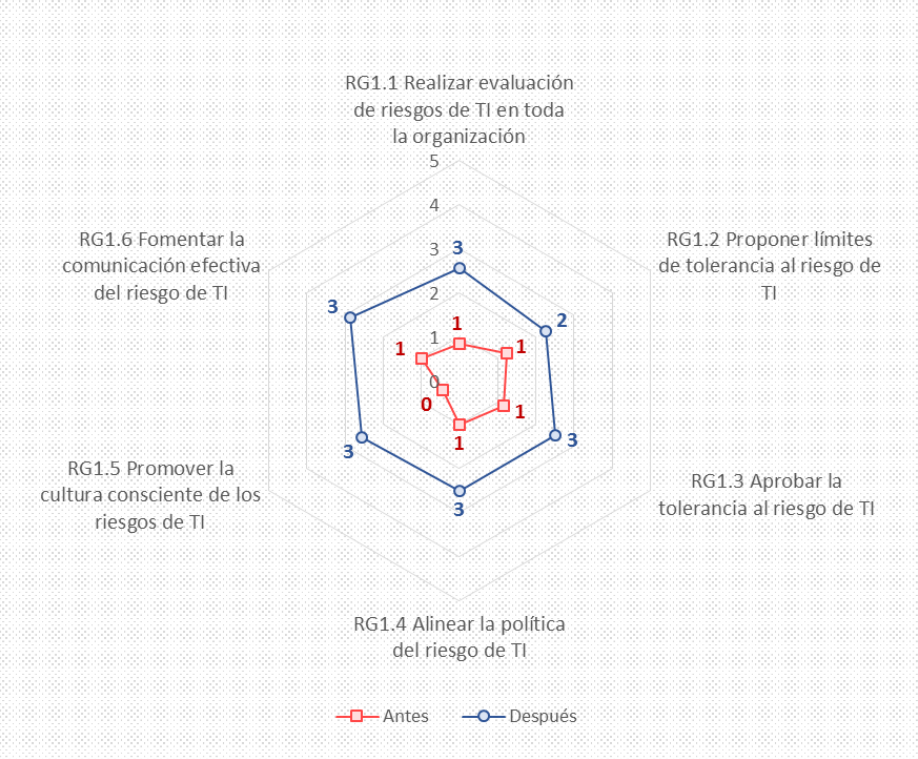
A continuación se presentan e interpretan los resultados obtenidos de la encuesta sobre el Modelo de Madurez para la Gestión de Riesgos de Tecnologías de Información en el periodo Diciembre 2014 a Diciembre 2015 en la Caja Rural de Ahorro y Crédito “Los Andes” S.A., dichos resultados fueron segmentados de acuerdo a los indicadores establecidos para la medición de la variable dependiente de la presente investigación.

4.2.1. RESULTADOS DEL INDICADOR "GOBIERNO DEL RIESGO"

El presente indicador cuenta con 3 procesos y 16 actividades, los cuales se evaluaron a través de 100 preguntas en la encuesta del Modelo de Madurez; los resultados por actividades, procesos e indicador son descritos a continuación:

Los resultados del proceso RG1 "Establecer y mantener una visión común del riesgo" revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 1, de los cuales se observa que en el periodo Diciembre 2015 a veces se proponían límites de tolerancia al riesgo de TI, asimismo de forma frecuente se realizaban evaluaciones de riesgos de TI en toda la organización, se aprobaba la tolerancia al riesgo de TI, se alineaba la política del riesgos de TI, se promovía la cultura consciente de los riesgos de TI y se fomentaba la comunicación efectiva del riesgo de TI.

Gráfico 1: Comparativo de Nivel de Madurez del Proceso RG1-Establecer y mantener una visión común del riesgo

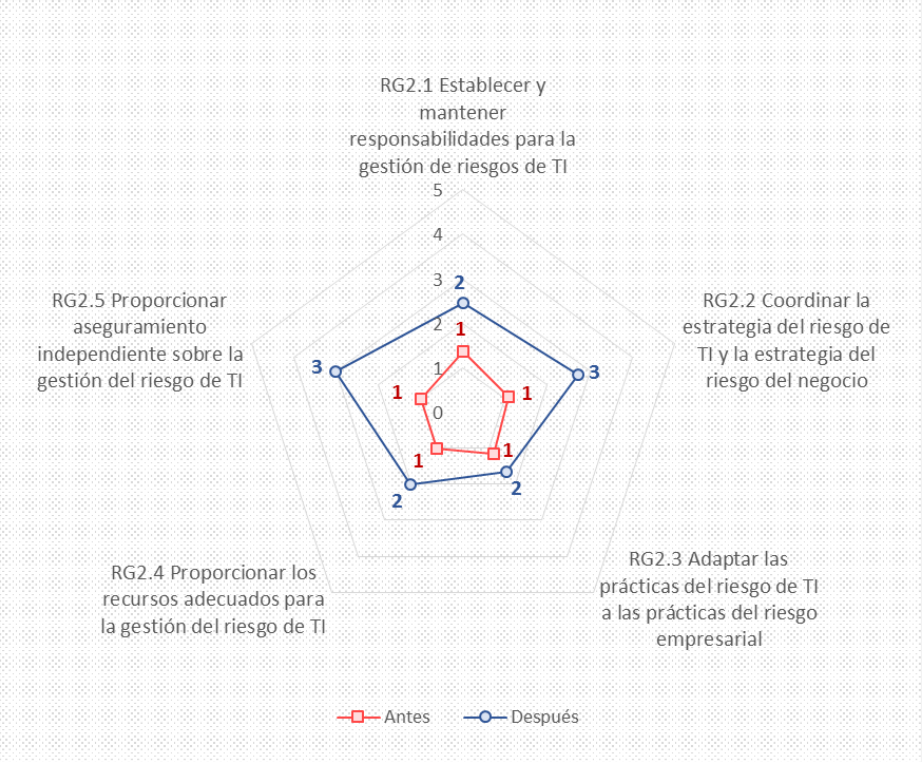


Elaboración: Propia

Los resultados del proceso RG2 “Integrar con la Gestión de Riesgos Empresariales” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 es Repetible (Nivel 2), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 2, de los cuales se observa que en el periodo Diciembre 2015 a veces se establecían y mantenían responsabilidades para la gestión de riesgos de TI, además se adaptaban las prácticas del riesgo de TI a las prácticas del riesgo empresarial y se proporcionaban los recursos adecuados para la gestión del riesgo de TI, así también de forma frecuente se coordinaba la estrategia del riesgo de TI y la estrategia del

riesgo del negocio y además se proporcionaba un aseguramiento independiente sobre la gestión del riesgo de TI.

Gráfico 2: Comparativo de Nivel de Madurez del Proceso RG2-Integrar con la Gestión de Riesgos Empresariales

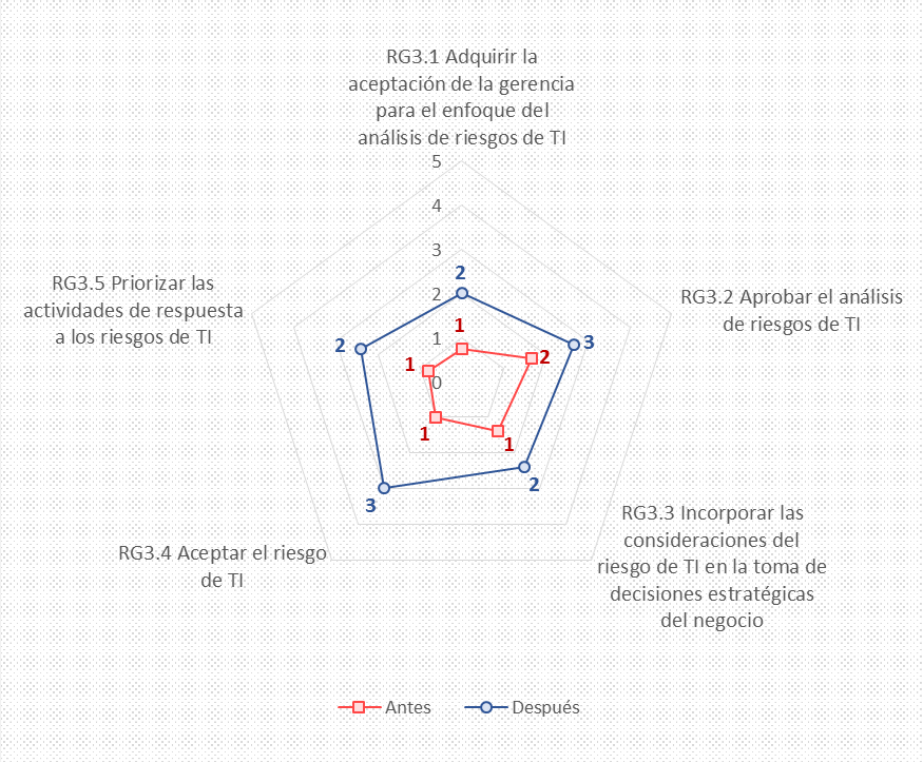


Elaboración: Propia

Los resultados del proceso RG3 “Tomar decisiones del negocio con conciencia del riesgo” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 es Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 3, de los cuales se observa que en el periodo Diciembre 2015 a veces se adquiría la aceptación de la gerencia para el enfoque del análisis de riesgos de TI, además se incorporaba las consideraciones del riesgo de TI en la toma de decisiones estratégicas del negocio y se priorizaban las actividades de

respuesta a los riesgos de TI, asimismo de forma frecuente se aprobaba el análisis de riesgos de TI y se aceptaba el riesgo de TI.

Gráfico 3: Comparativo de Nivel de Madurez del Proceso RG3-Tomar decisiones del negocio con conciencia del riesgo

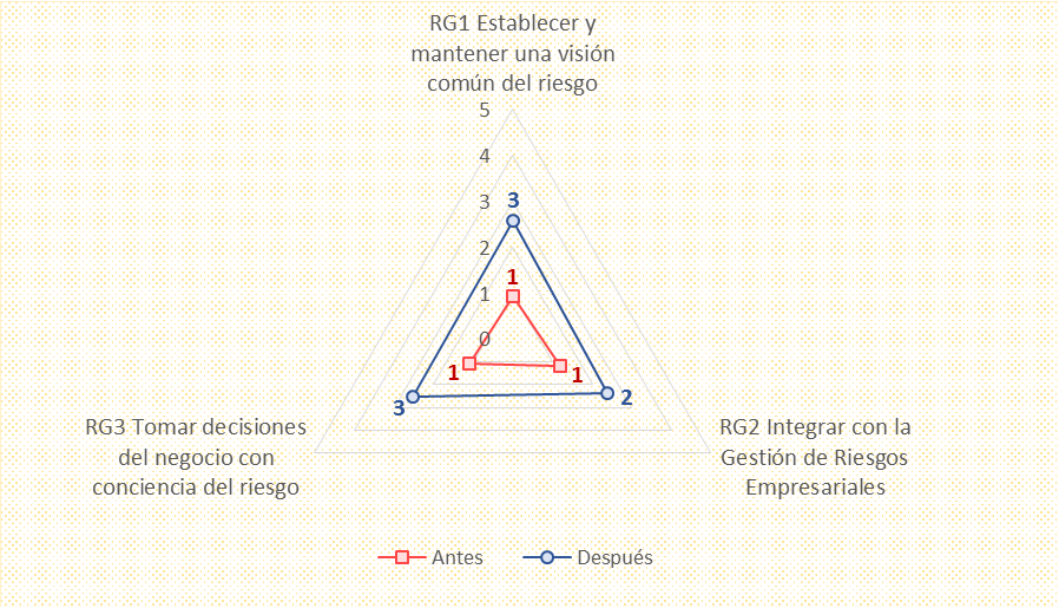


Elaboración: Propia

Los resultados del indicador RG "Gobierno del Riesgo" revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo en el periodo Diciembre 2015 el nivel de madurez es Repetible (Nivel 2), el resumen de los resultados por proceso se puede apreciar en el Gráfico 4, dichos resultados muestran que había una conciencia de la necesidad de controlar activamente los riesgos de TI, pero la atención se centraba en el cumplimiento técnico sin previsión del valor añadido; habiendo líderes emergentes para la gestión de riesgos de TI dentro de los departamentos quienes asumían la responsabilidad y solían ser considerados

responsables, incluso si no hay un acuerdo formal; la tolerancia del riesgo se establecía a nivel local y podía ser difícil de agregar; las inversiones estaban centradas en cuestiones de riesgo específico, dentro de los departamentos funcionales y de negocio (por ejemplo, seguridad, continuidad del negocio, operaciones); había necesidad de orientación de la junta directiva para la gestión de riesgos; requisitos de formación mínimos, que incluían una toma de conciencia de los riesgos de TI para zonas de riesgos críticos de la empresa; existían inventarios funcionales y departamentales de TI sobre cuestiones de riesgo.

Gráfico 4: Comparativo de Nivel de Madurez del Indicador RG-Gobierno del Riesgo



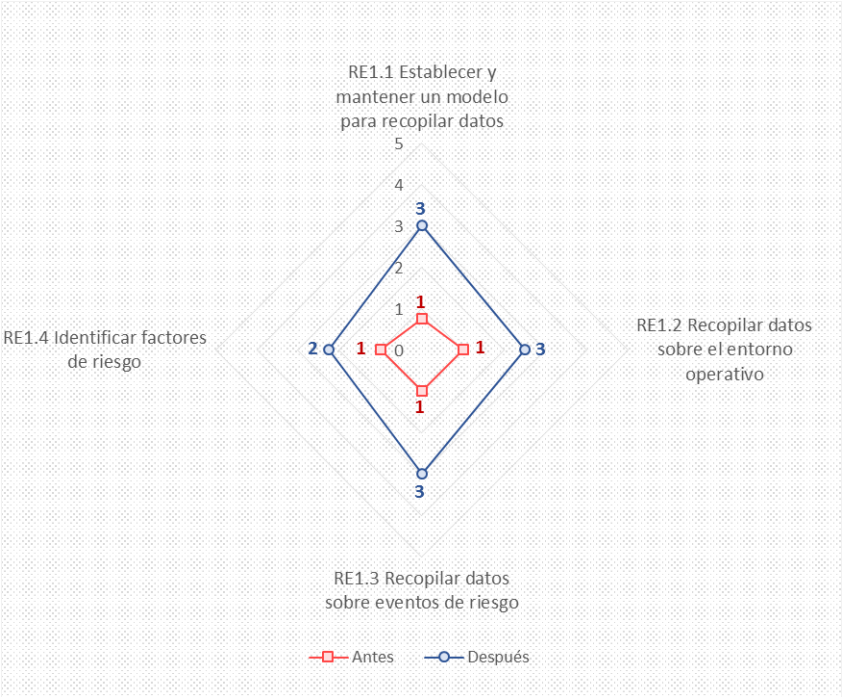
Elaboración: Propia

4.2.2. RESULTADOS DEL INDICADOR "EVALUACIÓN DEL RIESGO"

El presente indicador cuenta con 3 procesos y 14 actividades, los cuales se evaluaron a través de 55 preguntas en la encuesta del Modelo de Madurez; los resultados por actividades, procesos e indicador son descritos a continuación:

Los resultados del proceso RE1 “Recopilar datos” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 5, de los cuales se observa que en el periodo Diciembre 2015 a veces se identificaban factores de riesgo, asimismo de forma frecuente se establecía y mantenía un modelo para recopilar datos, además se recopilaban datos sobre el entorno operativo y se recopilaban datos sobre eventos de riesgo.

Gráfico 5: Comparativo de Nivel de Madurez del Proceso RE1-Recopilar datos

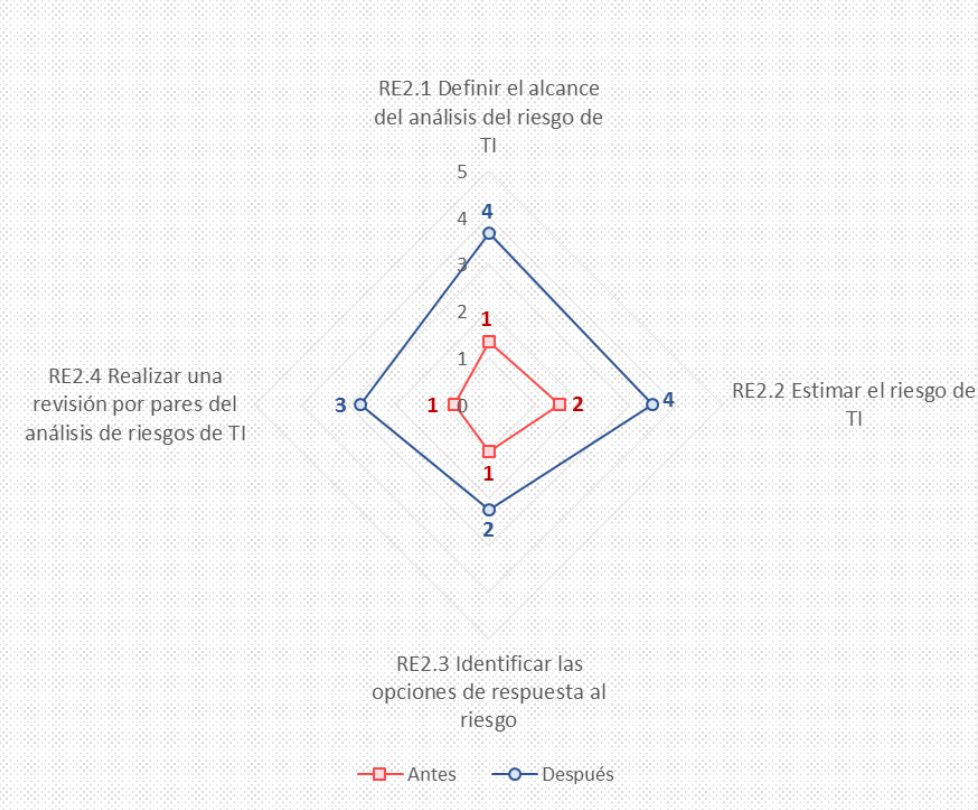


Elaboración: Propia

Los resultados del proceso RE2 “Analizar el riesgo” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 6, de los cuales se observa que en el periodo Diciembre

2015 a veces se identificaban las opciones de respuesta al riesgo, así también de forma frecuente se realizaba una revisión por pares del análisis de riesgos de TI y casi siempre se definía el alcance del análisis del riesgo de TI y su estimación.

Gráfico 6: Comparativo de Nivel de Madurez del Proceso RE2-Analizar el riesgo

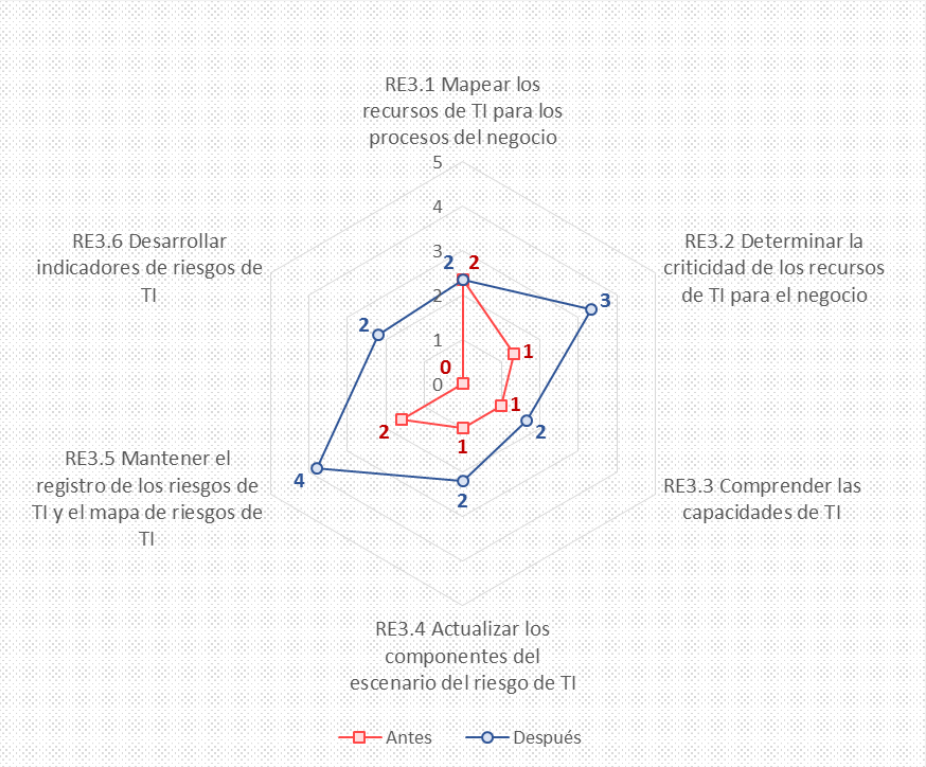


Elaboración: Propia

Los resultados del proceso RE3 “Mantener el perfil de riesgo” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 es Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 7, de los cuales se observa que en el periodo Diciembre 2015 a veces se mapeaban los recursos de TI para los procesos del negocio, además se comprendían las capacidades de TI, se actualizaban los componentes del escenario del riesgo

de TI y se desarrollaban indicadores de riesgos de TI, asimismo de forma frecuente se determinaba la criticidad de los recursos de TI para el negocio y casi siempre se mantenía el registro de los riesgos de TI y el mapa de riesgos de TI.

Gráfico 7: Comparativo de Nivel de Madurez del Proceso RE3-Mantener el perfil de riesgo

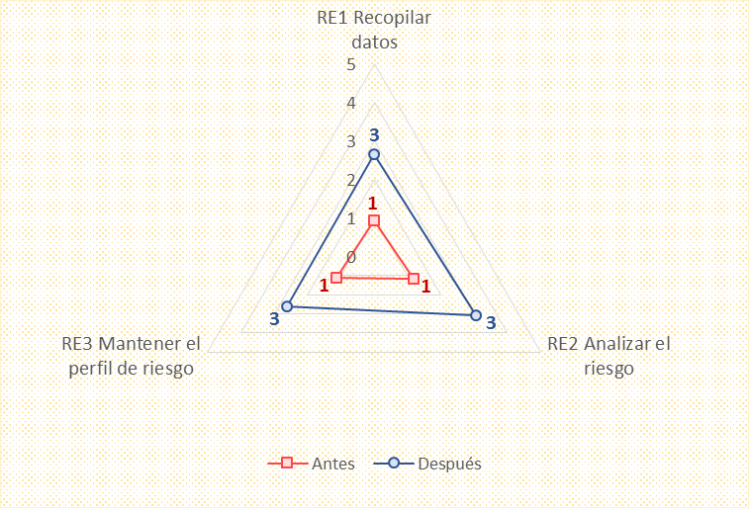


Elaboración: Propia

Los resultados del indicador RE "Evaluación del Riesgo" revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), el resumen de los resultados por proceso se puede apreciar en el Gráfico 8, dichos resultados muestran que había una comprensión de los fundamentos de los riesgos emergentes; las diferencias entre las TI y los riesgos relacionados con la oportunidad y el apetito de riesgo global eran reconocidos; la responsabilidad y rendición

de cuentas de las prácticas fundamentales de la evaluación de riesgo se definía y los dueños del proceso habían sido identificados; la capacidad estaba en el lugar para evaluar los riesgos de TI en conjunto con todos los tipos de riesgo; el análisis de dependencia y los procedimientos de análisis de escenarios se definían y se realizaban a través de actividades múltiples, las líneas de negocio y productos; las necesidades de competencias para todas las áreas de riesgo empresarial se encontraban definidos y documentados con plena consideración de la recopilación de datos, análisis de riesgos y perfiles; los instrumentos de recolección de datos generalmente se adherían a los estándares definidos y se distinguían entre los acontecimientos de amenaza, los acontecimientos de vulnerabilidad y acontecimientos de pérdida.

Gráfico 8: Comparativo de Nivel de Madurez del Indicador RE-Evaluación del Riesgo



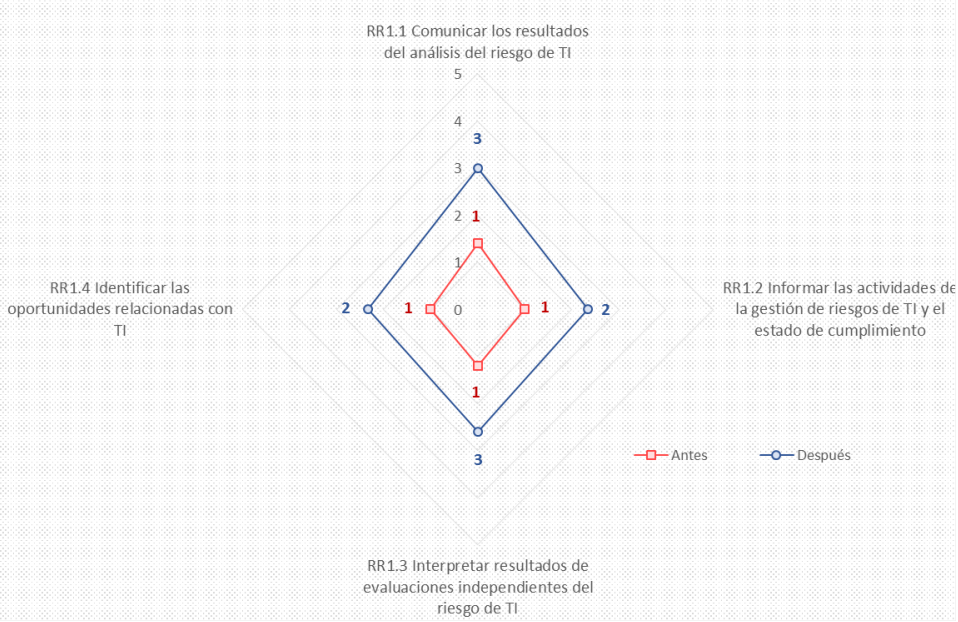
Elaboración: Propia

4.2.3. RESULTADOS DEL INDICADOR "RESPUESTA AL RIESGO"

El presente indicador cuenta con 3 procesos y 13 actividades, los cuales se evaluaron a través de 54 preguntas en la encuesta del Modelo de Madurez; los resultados por actividades, procesos e indicador son descritos a continuación:

Los resultados del proceso RR1 “Articular el riesgo” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 9, de los cuales se observa que el nivel de madurez en el periodo Diciembre 2015 a veces se informaban las actividades de la gestión de riesgos de TI y su estado de cumplimiento, además se identificaban las oportunidades relacionadas con TI, asimismo de forma frecuente se comunicaban los resultados del análisis de riesgo y se interpretaban resultados de evaluaciones independientes de riesgo de TI.

Gráfico 9: Comparativo de Nivel de Madurez del Proceso RR1-Articular el riesgo

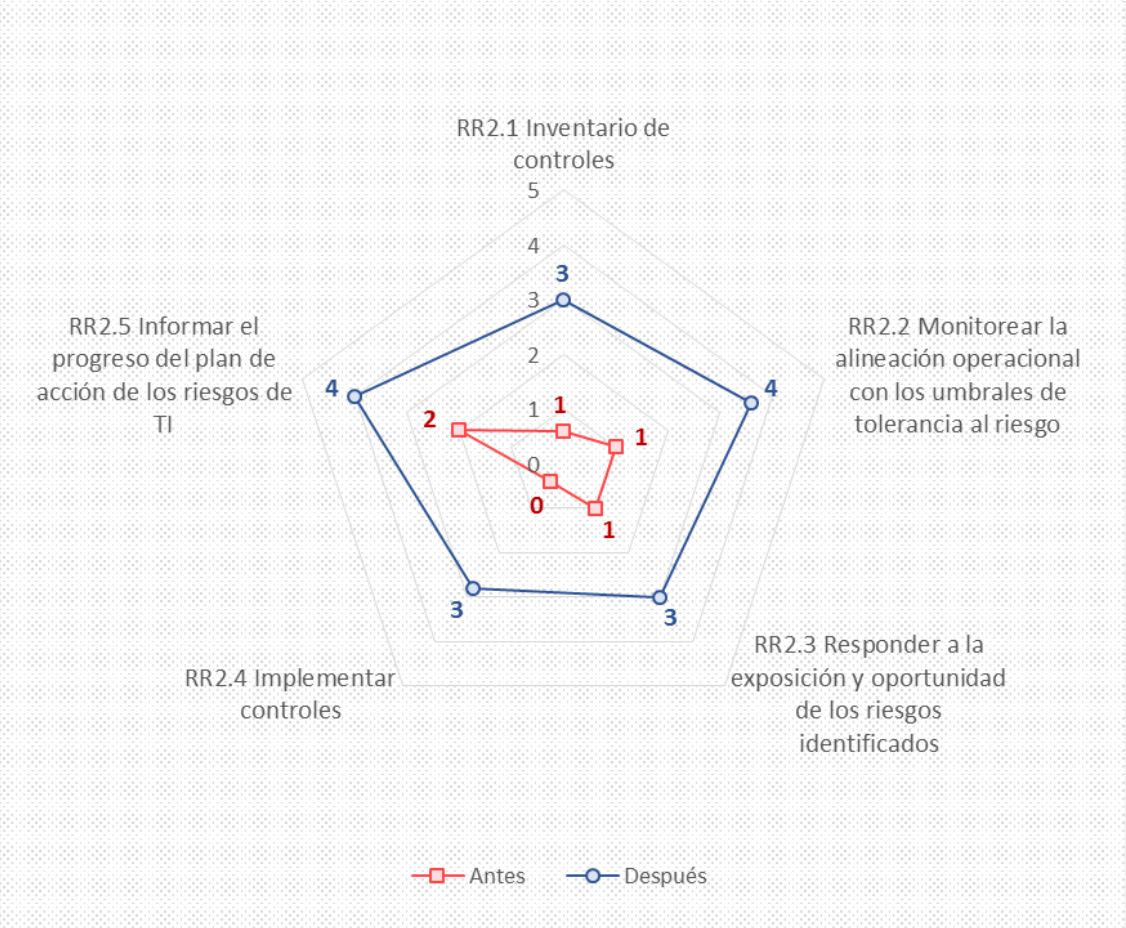


Elaboración: Propia

Los resultados del proceso RR2 “Gestionar el riesgo” revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 10, de los cuales se observa que en el periodo

Diciembre 2015 de forma frecuente se mantenía un inventario de controles, se respondía a la exposición y oportunidad de los riesgos identificados y además se implementaban controles, asimismo casi siempre se monitoreaba la alineación operacional con los umbrales de tolerancia al riesgo y se informaba el progreso del plan de acción de los riesgos de TI.

Gráfico 10: Comparativo de Nivel de Madurez del Proceso RR2-Gestionar el riesgo

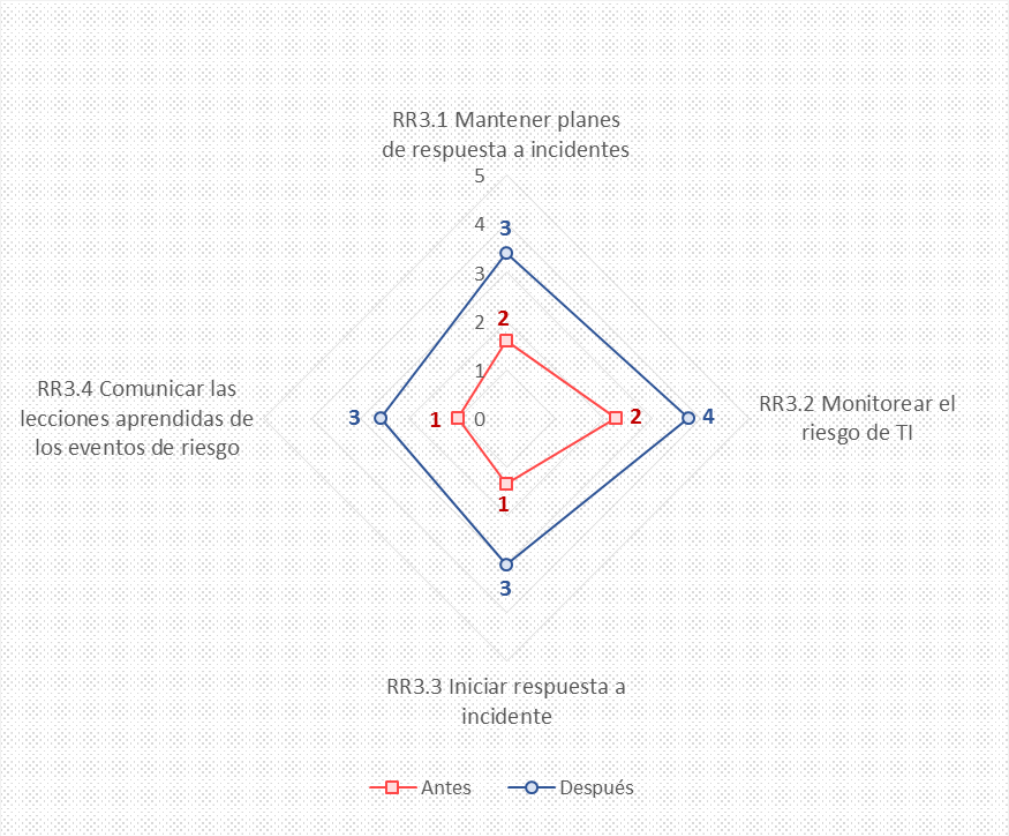


Elaboración: Propia

Los resultados del proceso RR3 “Reaccionar ante eventos” revelan que el nivel de madurez en el periodo Diciembre 2014 era Repetible (Nivel 2), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), los detalles de los resultados de las actividades del proceso se pueden apreciar en el Gráfico 11, de los cuales se observa que en el

periodo Diciembre 2015 de forma frecuente se mantenían planes de respuesta a incidentes, además se daba inicio a respuestas a incidentes y se comunicaba las lecciones aprendidas de los eventos de riesgo, asimismo casi siempre se monitoreaba el riesgo de TI.

Gráfico 11: Comparativo de Nivel de Madurez del Proceso RR3-Reaccionar ante eventos

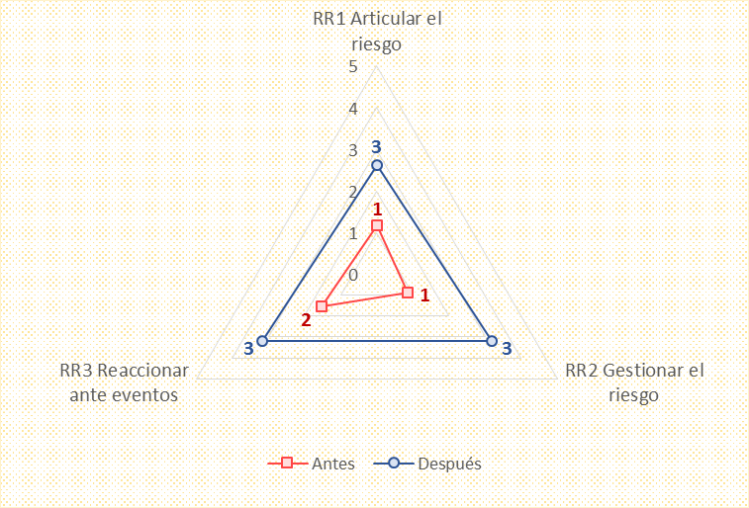


Elaboración: Propia

Los resultados del indicador RR "Respuesta al Riesgo" revelan que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), el resumen de los resultados por proceso se puede apreciar en el Gráfico 12, dichos resultados muestran que a través de la organización había comprensión individual del impacto de las amenazas de negocio y las acciones específicas a

tomar en caso de que se materializaran dichas amenazas; se definió responsabilidad y rendición de cuentas para las prácticas de respuesta clave de riesgo y los dueños del proceso fueron identificados; las deficiencias de control fueron identificadas y tratadas de manera oportuna; se definió cuándo y cómo responder a los riesgos en la política de respuesta a los riesgos; las descripciones de trabajo incluyeron las expectativas de respuesta a los riesgos; los empleados fueron capacitados periódicamente en amenazas relacionadas de TI, los escenarios de riesgo, y los controles pertinentes a sus funciones y responsabilidades; el plan fue definido para su uso y normalización de las herramientas para automatizar las actividades de reducción del riesgo, como el aprovisionamiento de usuarios.

Gráfico 12: Comparativo de Nivel de Madurez del Indicador RR-Respuesta al Riesgo



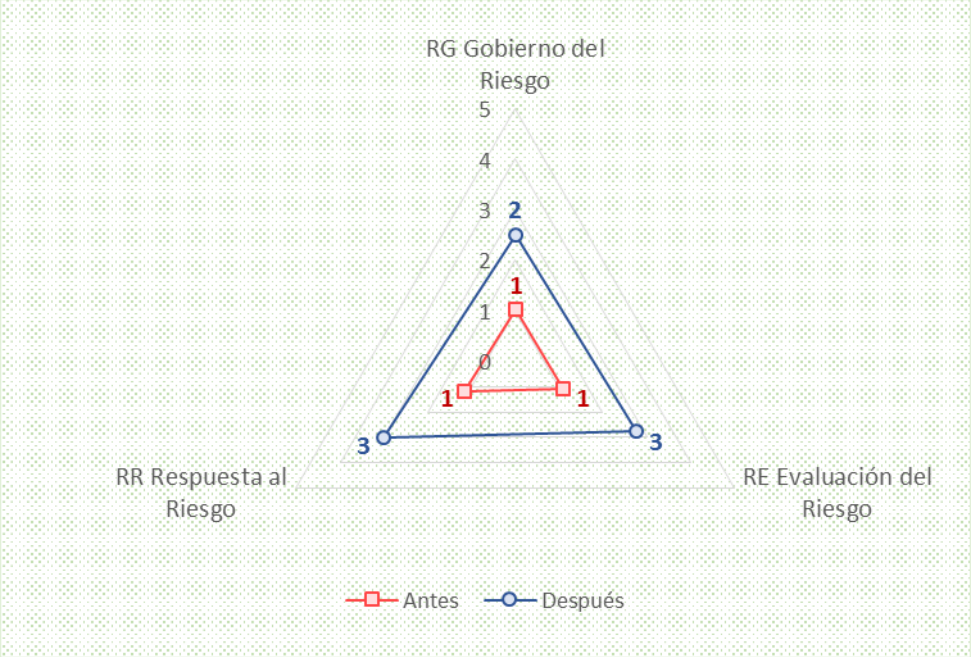
Elaboración: Propia

4.2.4. RESULTADOS GENERALES DE LA GESTIÓN DE RIESGOS DE TI

En el Gráfico 13 se puede observar el comparativo de los niveles de madurez de los tres indicadores (dominios) establecidos para la Gestión de Riesgos de Tecnología de Información

en la Caja Rural de Ahorro y Crédito "Los Andes" S.A. en los periodos Diciembre 2014 a Diciembre 2015.

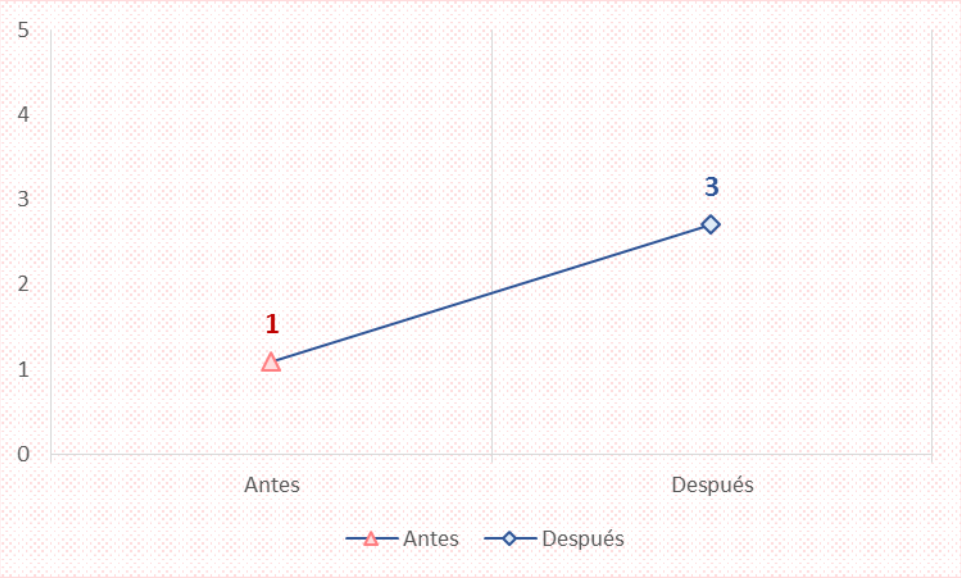
Gráfico 13: Comparativo de Nivel de Madurez de los Indicadores



Elaboración: Propia

En el Gráfico 14 se puede apreciar el resultado general de la Gestión de Riesgos de TI, el cual revela que el nivel de madurez en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 fue Definido (Nivel 3), con lo cual en el siguiente párrafo se describirá la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito "Los Andes" S.A. en el periodo Diciembre 2015.

Gráfico 14: Comparativo de Nivel de Madurez



Elaboración: Propia

Dicho resultado general muestra que en la Caja Rural de Ahorro y Crédito "Los Andes" S.A. en el periodo Diciembre 2015 se tenía consciencia de las amenazas y además se comprendía el impacto que representaban para el negocio y las acciones concretas que debían realizarse si el riesgo llegara a materializarse. Los procesos se encontraban debidamente documentados y eran comunicados a los diferentes niveles de la organización, asimismo, se encontraban estandarizados de tal forma que aplicaban para todo proyecto.

Los procesos se encontraban claramente definidos e incluían el propósito, entradas, criterios de entrada, actividades, roles, medidas, pasos de verificación, salidas y criterios de salida, asimismo eran manejados proactivamente entendiendo las interrelaciones de las actividades y medidas detalladas del proceso, sus artefactos y sus servicios.

Se identificaban los dueños de los procesos claves y se establecían responsabilidades para la comunicación de las respuestas al riesgo. Al identificar las deficiencias en controles, estas

eran corregidas de forma oportuna; se incluía dentro de la política de la empresa los procedimientos para respuesta al riesgo y esto se llegaba a definir a nivel de puestos de trabajo para que se tengan claras las expectativas de respuesta al riesgo.

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

4.3. DISCUSIÓN DE RESULTADOS

Esta investigación tuvo como propósito "Describir el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015".

De los resultados obtenidos en esta investigación se concluyó indicando que el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en el periodo Diciembre 2015 es Definido (Nivel 3), la descripción de este nivel de madurez a partir de la aplicación del Marco de Trabajo RISK IT ayudó a una mejor gestión del riesgo tecnológico minimizando su exposición, por lo que se afirma que a mayor nivel de madurez menores pérdidas que impacten en el negocio.

Esta investigación se relaciona con lo concluido por (Gualim Ac, 2014) puesto que se indica que el Marco de Referencia RISK IT es una herramienta útil para cualquier empresa que permite adaptarse de acuerdo a las necesidades, niveles de tolerancia y recursos que tiene la empresa, asimismo este Marco de Trabajo ayudó a proveer un plan de acción para minimizar la exposición al riesgo tecnológico.

Por otro lado, esta investigación también se relaciona con lo concluido por (Montenegro Hoyos & Riveras, 2011), puesto que esta investigación evidenció que la industria de software en general es de alto riesgo y de ahí la importancia de definir y realizar un proceso adecuado para gestión de los mismos, para lo cual se utilizó el Marco de Trabajo RISK IT el cual permitió una mejor gestión del riesgo tecnológico.

Se relaciona también con lo concluido por (López Marcos, 2011), dicha investigación indica que la gestión de riesgos de TI en las organizaciones sirve para evitar y minimizar pérdidas, pero también es útil para generar valor por medio de la aplicación de conceptos, principios y un conjunto de acciones definidas en controles, las cuales se definen como respuestas a estos riesgos, los cuales involucran la implementación del proceso de mejora continua del nivel de madurez, asimismo en esta investigación se indica que en el medio corporativo guatemalteco el nivel de madurez de la gestión de riesgos de TI es aceptable (Nivel 2).

Finalmente, se relaciona también con indicado por (Coronel Hoyos, 2008), dicha investigación concluye indicando que las etapas y actividades planteadas para la metodología de evaluación del riesgo tecnológico, permitieron alcanzar los objetivos propuestos, asimismo el plan piloto en el que se aplicó la metodología propuesta para la evaluación del riesgo tecnológico, permitió determinar que de su aplicación se obtienen resultados consistentes con la realidad de la institución evaluada, utilizando una de las mejores prácticas en administración de la tecnología de información, como lo es el marco de trabajo COBIT.

Por lo tanto, en base a la comparación de los resultados encontrados, podemos concluir que una buena gestión de riesgos de tecnología de información permite minimizar la exposición de estos y por lo tanto permite evitar pérdidas financieras, para conseguir esto es importante

utilizar una metodología que contenga procesos a seguir, asimismo es importante medir el nivel de gestión de riesgos de tecnología a partir de un modelo de madurez cada cierto periodo de tiempo para así identificar brechas e implementar mejoras, dichas conclusiones abordadas fueron incluidas en la presente investigación y también en los cuatro antecedentes mencionados.

CONCLUSIONES

PRIMERO: El nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes S.A. en el periodo Diciembre 2014 ha reflejado un nivel Inicial (Nivel 1), lo cual significa que los procesos eran Ad Hoc y desorganizados; asimismo en el periodo Diciembre 2015 el nivel reflejado fue Definido (Nivel 3), dicho nivel denota que los procesos son documentados y comunicados, mostrando una frecuencia de cumplimiento de 4 (Frecuentemente) de un total de 6 (Siempre). Toda empresa dependiente de TI para la gestión de sus operaciones, está expuesta a diversos factores de riesgo que va en relación al nivel de dependencia que tienen en TI; su mitigación está dada en base a las acciones, respuestas, planes y proyectos que implemente para incrementar el nivel de madurez que poseen para la gestión de riesgos, mientras más dependientes de TI mayor será la exposición al riesgo, por tanto a mayor nivel de madurez menores pérdidas que impacten en el negocio.

SEGUNDO: Con respecto al primer objetivo específico se concluye que, el nivel de madurez del dominio "Gobierno del Riesgo" en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 era Repetible (Nivel 2), el nivel de madurez de este último periodo significa que las prácticas de la Gestión de Riesgos de TI se habían integrado en la empresa, permitiendo obtener un rendimiento óptimo del riesgo con una frecuencia de cumplimiento de 3 (A Veces) de un total de 6 (Siempre), además indica que los procesos seguían un patrón regular.

TERCERO: Con respecto al segundo objetivo específico se concluye que, el nivel de madurez del dominio "Evaluación de Riesgos" en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 era Definido (Nivel 3), el nivel

de madurez de este último periodo significa que los riesgos y oportunidades relacionados a TI eran identificados, analizados y presentados en términos del negocio con una frecuencia de cumplimiento de 4 (Frecuentemente) de un total de 6 (Siempre), además indica que los procesos eran documentados y comunicados.

CUARTO: Con respecto al tercer objetivo específico se concluye que, el nivel de madurez del dominio "Respuesta a los Riesgos" en el periodo Diciembre 2014 era Inicial (Nivel 1), asimismo el nivel de madurez en el periodo Diciembre 2015 era Definido (Nivel 3), el nivel de madurez de este último periodo significa que los problemas, oportunidades y eventos de riesgo relaciones a TI fueron dirigidos de una manera rentable y en línea con las prioridades del negocio con una frecuencia de cumplimiento de 4 (Frecuentemente) de un total de 6 (Siempre), además indica que los procesos fueron documentados y comunicados.

SUGERENCIAS

PRIMERO: Se sugiere difundir información acerca de la importancia de la Gestión de Riesgos de Tecnología de Información, ya que es fundamental su aplicación en todas las empresas de todos los rubros.

SEGUNDO: Se sugiere aplicar de forma anual la encuesta del modelo de madurez establecido para monitorear el nivel de la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito “Los Andes” S.A.

BIBLIOGRAFÍA

Amutio Gómez, M. A., Candau, J., & Mañas, J. A. (2012). *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (Tercera Edición ed.). Madrid: Ministerio de Hacienda y Administraciones Públicas. doi:630-12-171-8

AS. (1999). *Estándar Australiano AS/NZS 4360:1999.*

Committee of Sponsoring Organizations of the Treadway Commission. (1992). *COSO I.*

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *COSO ERM.*

Coronel Hoyos, K. D. (2008). *Metodología de Evaluación del Riesgo Tecnológico en las Instituciones del Sistema Financiero Ecuatoriano, utilizando COBIT 4.1*. Ecuador.

Ernst & Young. (2012). Cambios en el panorama de los riesgos de TI. *Perspectivas sobre los riesgos de TI*, 16.

Facultad de Ciencias Administrativas de la Universidad Nacional Mayor de San Marcos. (2009). Los Procesos de Gestión. *Gestión en el Tercer Milenio*, 5.

Fischer, U. (01 de Julio de 2010). *ISACA.* Obtenido de http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Publica-en-Espa%C3%B1olel-Marco-de-RiesgosdeTIparaAyudaralasOrganizacionesa-Obtener-Beneficios-y-a-Mitigar-los-Riesgos.aspx

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

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2013). *Metodología de la Investigación* (Quinta Edición ed.). México: The McGraw-Hill Companies.

Hildago Nuchera, A. (01 de Enero de 2014). *Una introducción a la gestión de riesgos tecnológicos.* (U. P. Madrid, Ed.) Obtenido de Una introducción a la gestión de riesgos tecnológicos: http://www.madrimasd.org/revista/revista23/tribuna/tribuna1.asp

ISACA. (2009). *Marco de Riesgos de TI.* Orlando, Florida, USA: Rolling Meadows. doi:978-1-60420-111-6

ISO 31000:2009. (Diciembre de 2009). *ISO International Organization for Standardization*. Obtenido de https://www.iso.org/standard/43170.html

Kaplan, S., & Garrick, B. (1981). *On the quantitative definition of risk.* Houston: Risk Analisys.

López Marcos, N. E. (2011). *Gestión de Riesgos Corporativos de TI en Guatemala.* Guatemala.

Mitacc Meza, M. (2011). *Tópicos de Estadística Descriptiva.* Lima, Perú: THALES S.R.L.

Montenegro Hoyos, J. J., & Riveras, R. M. (2011). *RISK IT como complemento a la Gestión de Riesgos en compañías de la industria de software.* Colombia.

Puy, A. (1995). *Percepción social de los riesgos.* Madrid: Mapfre.

Real Academia Española. (2017). *Diccionario de la Lengua Española*. Obtenido de Diccionario de la Lengua Española: http://dle.rae.es/

Roig, F. (Abril de 2015). *WEIB.* Obtenido de WEIB: http://weib.caib.es/Recursos/tic/tic_conceptes.pdf

Superintendencia de Banca y Seguros, S. (2008). *Resolución SBS N° 37-2008.* Lima.

Superintendencia de Banca y Seguros, S. (2009). *Resolución SBS Nº 2116-2009.* Lima.

Valle, R., Ros, F., Barberá, J., & Gamella, M. (1986). *Los países industrializados ante las nuevas tecnologías, FUNDESCO.* Madrid: ETSI.

Westerman, H. (2007). *IT Risk: Turning Business Threats Into Competitive Advantage.* USA: Harvard Business School Press.

Young, N. (05 de Mayo de 2014). *Gestión*. Obtenido de http://gestion.pe/empresas/pwc-empresas-actualmente-se-encuentran-mas-preocupadas-cambios-tecnologicos-y-riesgos-ti-2096255

ANEXOS

Anexo 1: Encuesta del Modelo de Madurez

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
RK	**Marco de Trabajo RISK IT**							**1**							**3**
RG	**Gobierno del Riesgo.**							**1**							**2**
RG1	**Establecer y mantener una visión común de riesgo.**							**1**							**3**
RG1.1	**Realizar evaluación de riesgos de TI en toda la organización.**							**1**							**3**
1	¿Se realizan talleres para determinar el nivel de riesgo que la organización está dispuesta a aceptar en el camino hacia la consecución de sus objetivos estratégicos?	X						0				X			3
2	¿La administración de TI ayuda a la empresa a comprender los riesgos de TI en el contexto de escenarios que afectan el negocio y sus objetivos estratégicos (P. Ej.: Ventas, Costos, Satisfacción del Cliente, Dinero)		X					1			X				2
3	¿Se realiza un análisis top-down, end-to-end de los servicios empresariales para determinar los principales puntos de soporte de TI?		X					1			X				2
4	¿Se realiza un análisis para identificar dónde se genera valor, dónde debe ser protegido y ser sostenido?		X					1		X					1
5	¿Se identifican eventos relacionados con las TI y las condiciones que pueden poner en riesgo el valor, afectar el desempeño de la empresa y la ejecución de actividades críticas del negocio dentro de parámetros aceptables o que de otro modo afectan los objetivos de la empresa (P. Ej.: negocios, regulatorios, jurídicos o legales, contratos, tecnológicos, socios comerciales, recursos humanos, otros aspectos operacionales)		X					1					X		4
6	¿Se elabora un mapa de riesgos impulsado por el negocio la cual categoriza y subcategoriza los riesgos derivados de los escenarios de riesgo de TI de alto nivel?		X					1							
7	¿Se dividen los riesgos de TI por líneas de negocio, producto, servicio y procesos?	X						0			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
8	¿Se identifican posibles riesgos en cascada, los tipos de amenaza y se analiza la causa-efecto probable de su concentración y su correlación?		X					1				X			3
9	¿Se entiende como las capacidades de TI contribuyen a la capacidad de la empresa para añadir valor y soportar la pérdida?			X				2				X			3
10	¿Se analiza la percepción de la gerencia sobre la importancia de las capacidades de TI en su estado actual?	X						0		X					1
11	¿Se toma en consideración cómo la estrategia de TI, iniciativas de cambio y requisitos externos (P. Ej.: regulaciones, contratos, normas o estándares industriales, entre otros) pueden afectar el perfil de riesgos?		X					1				X			3
12	¿Se identifica dónde se concentran las zonas de riesgo, los escenarios, las dependencias, los factores de riesgo y medidas de riesgo que requieren atención para posteriormente ser analizados y desarrollados?		X					1					X		4
RG1.2	**Proponer límites de tolerancia al riesgo de TI.**							**1**							**2**
13	¿Se establece los niveles de riesgos relacionados con TI que está dispuesto a tolerar para cumplir sus objetivos, a nivel de una línea de negocio, producto, servicio, proceso?		X					1				X			3
14	¿Se definen límites en medidas similares a los objetivos del negocio subyacentes y en contra de los impactos del negocio aceptables e inaceptables?		X					1			X				2
15	¿Se toman en consideración compensaciones que pueden ser necesarias para alcanzar los objetivos clave en el contexto del equilibrio de riesgo/rentabilidad?			X				2			X				2
16	¿Se proponen límites y medidas en el contexto de la relación valor/beneficio de implantación de tecnología, programas y ejecución de proyectos de TI, operaciones y ejecución de servicios de TI a través de múltiples horizontes de tiempo (P. Ej.; de inmediato, corto plazo, largo plazo)?		X					1			X				2
RG1.3	**Aprobar la tolerancia al riesgo de TI.**							**1**							**3**

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
17	¿Se evalúan las propuestas de umbrales de tolerancia de riesgos frente a los riesgos aceptables de la empresa y los niveles de oportunidad?			X				2				X			3
18	¿Se toman en consideración los resultados de la evaluación de riesgos de TI en la empresa y las compensaciones necesarias para alcanzar los objetivos clave en el contexto del equilibrio de riesgo/rentabilidad?			X				2			X				2
19	¿Se toman en consideración los posibles efectos de la concentración de riesgos de TI y la correlación entre las líneas del negocio, productos, servicios y procesos?		X					1				X			3
20	¿Se evalúan los umbrales específicos de una unidad para determinar si estos deben aplicarse a todas las líneas del negocio?	X						0		X					1
21	¿Son definidos aquellos tipos de eventos (internos o externos) y cambios en los entornos del negocio o tecnologías, que pueden requerir una modificación a los niveles de tolerancia al riesgo de TI?		X					1				X			3
22	¿Son aprobados los umbrales de tolerancia al riesgo de TI por los responsables de la gestión de riesgos?		X					1				X			3
RG1.4	**Alinear la política del riesgo de TI.**							**1**							**3**
23	¿Se incluye el apetito y tolerancia en la política del riesgo tecnológico a todos los niveles de la empresa?		X					1			X				2
24	¿Se reconoce que el riesgo de TI es inherente a los objetivos de la empresa y se documenta cuanto riesgo está dispuesta a asumir (nivel tolerancia) en búsqueda de lograr los objetivos?		X					1				X			3
25	¿Son documentados los principios de gestión de riesgos, las áreas de enfoque de riesgos y las mediciones clave?		X					1				X			3
26	¿Se ajusta la política de riesgos de TI basada en los cambios de las condiciones de riesgo y las amenazas emergentes?		X					1			X				2
27	¿Se encuentra alineada la política operacional y las normas o estándares con la tolerancia al riesgo?		X					1			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
28	¿Se realizan revisiones periódicas o provocadas, de la política operacional y las normas o estándares contra la política de riesgos de TI y la tolerancia?		X					1			X				2
29	¿Al identificar brechas, se establecen objetivos definiendo fechas basadas en los límites de tiempo de exposición al riesgo aceptables y los recursos necesarios?		X					1					X		4
30	¿Cuándo es necesario, se realizan ajustes a los niveles de tolerancia de riesgos en lugar de modificar la política operacional y estándares o normas establecidas?		X					1			X				2
RG1.5	**Promover la cultura consciente de los riesgos de TI.**							**0**							**3**
31	¿Se promueve una cultura de riesgo capacitando a la empresa para identificar riesgos, oportunidades e impactos potenciales de TI en el negocio de forma proactiva?		X					1				X			3
32	¿Los empleados son estimulados para hacer frente a problemas originados por riesgos de TI antes de que estos aumenten gravemente?		X					1					X		4
33	¿Se entrena al personal del negocio y de TI acerca de las amenazas, impactos y cómo reaccionar empleando respuestas planificadas ante eventos de riesgo específicos?	X						0			X				2
34	¿Se comunica a las áreas enfocadas al riesgo "el por qué debe cuidarse" y se explica cómo tomar acciones conscientes de los riesgos no especificados en la política de riesgos?	X						0			X				2
35	¿Se realizan ensayos de escenarios para áreas que no se encuentran cubiertas por la política de riesgos de TI y así reforzar las expectativas para comprender la dirección de la política general y el uso del sentido común?	X						0			X				2
36	¿Se fomenta el debate para definir el nivel apropiado de riesgo a aceptar por parte de la empresa?		X					1				X			3
37	¿Se promueve una cultura de gestión de riesgos tecnológicos alineada a la cultura de concientización de riesgos del negocio?	X						0			X				2
RG1.6	**Fomentar la comunicación efectiva del riesgo de TI.**							**1**							**3**

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
38	¿Se establece y mantiene un plan de comunicación de riesgos que cubre la política de riesgos de TI, responsabilidades, rendición de cuentas y el panorama de riesgos? (P. Ej.: las amenazas, los controles, el impacto, causas raíz, decisiones del negocio)		X					1				X			3
39	¿Se filtra las características del plan de tal modo que sea claro, conciso, útil y dirigido a la audiencia correcta?		X					1			X				2
40	¿Se realiza una comunicación frecuente y periódica entre la gestión de TI y la dirección del negocio para tratar la situación actual de los riesgos de TI, las preocupaciones o intereses y las exposiciones?		X					1				X			3
41	¿Se fomenta una comunicación y administración de TI con un enfoque que busca alinear los riesgos de TI con los riesgos del negocio?		X					1				X			3
42	¿Se fomenta una comunicación y administración de TI con un enfoque que busca priorizar periódicamente los riesgos de TI alineados a los riesgos del negocio?	X						0			X				2
43	¿Se fomenta una comunicación y administración de TI con un enfoque que busca expresar los riesgos de TI en términos estratégicos y operativos del negocio?		X					1				X			3
44	¿Se comunica claramente cómo los acontecimientos adversos relacionados con TI afectan los objetivos empresariales? (P. Ej.: objetivos del negocio, las categorías objetivo de COSO ERM)			X				2					X		4
45	¿Se fomenta una comunicación clara para que los altos ejecutivos y directivos de TI comprendan el nivel real de los riesgos de TI y así puedan asignar los recursos adecuados para responder a riesgos de TI alineados al apetito y tolerancia definidos?		X					1				X			3
RG2	**Integrar con la Gestión de Riesgos Empresariales.**							**1**							**2**
RG2.1	**Establecer y mantener responsabilidades para la gestión de riesgos de TI.**							**1**							**2**

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
46	¿Se tienen identificados los responsables y encargados de la gestión de riesgos de TI en toda la empresa?			X				2				X			3
47	¿A nivel de los altos ejecutivos y responsables de la gestión de riesgos de TI, se tienen establecidas las expectativas de incorporar la consciencia de riesgos a la cultura organizacional?		X					1			X				2
48	¿Se tienen definidos los indicadores de desempeño y procesos de presentación de informes con los niveles adecuados de reconocimiento, aprobación, incentivos y sanciones?			X				2				X			3
49	¿Existen estructuras definidas para involucrar al negocio en la toma de decisiones de riesgos y de las operaciones del día a día? (P. Ej.: Comité de riesgos del negocio, consejo de riesgos de TI, Oficial de riesgos de TI)				X			3				X			3
50	¿Se tienen definidas las funciones que diferencien las responsabilidades de las unidades de negocio (qué poseen y la gestión del riesgo en el día a día), control interno (que proveen expertos en la materia para evaluación y asesoramiento) y auditoria interna (que ofrecen una garantía independiente)?				X			3					X		4
51	¿Se tienen definidos los gerentes o directores del negocio con autoridad para tomar decisiones sobre riesgos de TI, beneficios y generación de valor por medio de las TI, programas y ejecución de proyectos de TI, así como operaciones y entrega de servicios de TI?					X		4					X		4
52	¿Se tienen definidas las expectativas para los administradores de las políticas, estándares o normas, controles y actividades de supervisión del cumplimiento (P. Ej.: Establecimiento y seguimiento de KRIs)?	X						0			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
53	¿Se establece y evalúa las metas de desempeño para evaluar el equilibrio del riesgo-retorno-concientización en la toma de decisiones? (P. Ej.: la capacidad de los administradores para integrar y equilibrar la gestión del desempeño con la gestión de riesgos a través de sus límites de autoridad)	X						0			X				2
54	¿Se tienen roles definidos para administrar dominios específicos de riesgos de TI? (P. Ej.: gestión de la capacidad de los sistemas, dotación personal de TI, selección y evaluación de sistemas o programas)	X						0			X				2
55	¿Se asigna a cada dominio un nivel de criticidad en función del riesgo?	X						0		X					1
56	¿De ser necesario, se asignan responsabilidades adicionales para la gestión de riesgos en niveles inferiores o requisitos externos? (P. Ej. Para sistemas específicos)	X						0		X					1
RG2.2	**Coordinar la estrategia del riesgo de TI y la estrategia del riesgo del negocio.**							**1**							**3**
57	¿La definición de la gestión de riesgos de TI se realiza en el contexto de la protección y mantenimiento de procesos del negocio o actividades empresariales?			X				2				X			3
58	¿El marco de riesgos de TI es alineado al marco existente para la gestión de riesgos del negocio?	X						0			X				2
59	¿Los aspectos o información específica de TI, son integrados en un enfoque empresarial?				X			3				X			3
60	¿Se tienen claras las metas y objetivos de riesgos empresariales así como la combinación de factores de riesgos que afectan a la empresa y las limitaciones de recursos?			X				2				X			3
61	¿Se define cómo debe abordarse la gestión de riesgos de TI en el contexto del ámbito de riesgos del negocio y otro tipo de riesgos empresariales?	X						0			X				2
62	¿Se tiene definido el papel del departamento de TI en la gestión del riesgo operacional, en función del grado de dependencia del negocio en TI y la infraestructura física, relacionada con el logro de objetivos financieros, operativos y satisfacción del cliente?			X				2				X			3

Continúa…

	CRITERIO DE EVALUACIÓN	ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
63	¿Se coordinan actividades de evaluación de riesgos y se presentan informes integrados?	X						0				X			3
64	¿Los riesgos que son identificados cuentan con escalas de calificación (p. ej.: frecuencia e impacto), categorías de control (p. ej.: preventivo, detectivo o correctivo) y tienen definidas jerarquías en función de políticas de riesgos, estándares o normas y, procedimientos?		X					1					X		4
65	¿Cuándo es posible, se emplean principios de ERM y puntos de vistas de riesgos existentes para la gestión del riesgo de TI? (p. ej.: desde el punto de vista actuarial, de cartera, de sistemas)		X					1				X			3
66	¿Se evalúa cómo y cuándo ciertos puntos de vista de riesgos del negocio pueden utilizarse para la gestión de riesgos de TI?		X					1			X				2
67	¿La estrategia de gestión de riesgos de TI satisface las necesidades de rendimiento de la empresa y de requerimientos externos?	X						0			X				2
RG2.3	**Adaptar las prácticas del riesgo de TI a las prácticas del riesgo empresarial.**							**1**							**2**
68	¿Los riesgos existentes son organizados para (1) entender el contexto del negocio de TI (p. ej.: actividades del negocio de TI, análisis de dependencias, análisis de escenarios), (2) identificar los riesgos de TI (p. ej.: modelos de datos, rutas de ajuste o escalamiento), (3) regular los riesgos de TI (p. ej.: procedimientos empresariales de evaluación de riesgos de TI, modelos de decisión en función del riesgo) y (4) gestionar los riesgos de TI (p. ej.: selección de los KRI's adecuados para el desempeño de los objetivos del negocio y definir procedimientos de escalamiento)?		X					1					X		4
69	¿Se comprenden las expectativas empresariales de la gestión de riesgos, actividades y métodos que son relevantes para la gestión de riesgos de TI? (p. ej.: gestión de problemas, comunicación y formación, cómo se miden e identifican los riesgos, cómo se evalúan los controles, qué información se proporciona y a quién, cómo se establece y acuerda el apetito de riesgo)			X				2			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
70	¿Se evalúan las prácticas de gestión de riesgos de TI para identificar brechas a minimizar para satisfacer las expectativas de la ERM?		X					1		X					1
71	¿Se identifican las actividades de la gestión de riesgos del negocio que deben agregarse o modificarse para alinearse a la gestión de riesgos de TI?		X					1		X					1
72	¿Continuamente se analizan qué otras funciones se realizan o deben realizarse en apoyo del cumplimiento de los objetivos del negocio y la gestión de riesgos de TI?		X					1		X					1
73	¿Se priorizan y se da seguimiento a los esfuerzos que se realizan para cerrar las brechas entre la gestión de riesgos de TI y ERM para mejorar la eficacia y eficiencia (p. ej.: optimizar controles, agilizar las evaluaciones de riesgos, coordinar KRI's, escalar desencadenadores, integración de informes)		X					1		X					1
RG2.4	**Proporcionar los recursos adecuados para la gestión del riesgo de TI.**							**1**							**2**
74	¿Se analizan las necesidades de recursos para la gestión de riesgos a nivel de TI como del negocio en el contexto de competencias, aspectos del negocio, limitaciones de recursos y objetivos?		X					1			X				2
75	¿Se asignan los fondos necesarios para cerrar las brechas y posicionar a la empresa para tomar ventaja competitiva de las oportunidades?		X					1			X				2
76	¿Se evalúa la criticidad del riesgo para intercambiar riesgo/beneficio de acuerdo a los objetivos organizacionales? (p.ej.: asignar más o menos recursos en base a la criticidad de los datos dentro de un procedimiento por etapas para seguridad informática)		X					1			X				2
RG2.5	**Proporcionar aseguramiento independiente sobre la gestión del riesgo de TI.**							**1**							**3**
77	¿Se supervisan los riesgos y se establecen planes de acción para garantizar el desempeño de las prácticas realizadas para la gestión de riesgos de TI y, se evalúa si estos se gestionan de acuerdo al apetito y tolerancia al riesgo?		X					1				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
RG3	**Tomar decisiones del negocio con conciencia del riesgo.**							**1**							**3**
RG3.1	**Adquirir la aceptación de la gerencia para el enfoque del análisis de riesgos de TI.**							**1**							**2**
78	¿El personal que toma decisiones es formado (instruido o capacitado) en el enfoque de análisis de riesgos de TI?		X					1			X				2
79	¿Se da a conocer cómo los resultados del análisis de riesgos puede beneficiar las decisiones importantes de la empresa?			X				2					X		4
80	¿Se define el nivel de calidad que se espera de quienes toman decisiones, cómo interpretar los informes de riesgos, la definición de términos clave (p. ej.: las probabilidades y factores de riesgo), las limitaciones de las mediciones y las estimaciones basadas en datos incompletos?	X						0		X					1
81	¿Se tienen identificadas las brechas del enfoque de análisis de riesgos con las expectativas del riesgo empresarial?	X						0		X					1
RG3.2	**Aprobar el análisis de riesgos de TI.**							**2**							**3**
82	¿Se analizan los informes de riesgos para determinar si estos proporcionan información útil para comprender los riesgos y de ser necesario, para evaluar las opciones de respuesta a los riesgos?			X				2					X		4
83	¿Para aprobar el análisis de riesgos de TI, se toma en cuenta las limitaciones que se tienen?		X					1		X					1
84	¿Los informes presentados de riesgos de TI, son analizados para que estos sean aprobados o rechazados?			X				2				X			3
RG3.3	**Incorporar las consideraciones del riesgo de TI en la toma de decisiones estratégicas del negocio.**							**1**							**2**
85	¿Regularmente se realiza un análisis de los factores de riesgo de TI previo a la toma de decisiones del negocio para que estos sean tomados en cuenta?		X					1			X				2
86	¿Se realiza un análisis del portafolio de aplicaciones en comparación con el valor que ofrecen los procesos del negocio para identificar oportunidades de mejora que tomen en consideración los riesgos, retorno y cambios previstos en el entorno de TI?		X					1			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
87	¿Se toma en consideración los efectos que tendrá en la gestión empresarial los riesgos de TI y la capacidad de la gestión de riesgos (controles, recursos, capacidades) sobre las decisiones empresariales y del negocio?			X				2				X			3
88	Como parte de la gestión empresarial, ¿Los riesgos de TI son comprendidos desde diversos puntos de vista del portafolio de servicios (p. ej.: unidades del negocio, producto, procesos) y se valora el impacto que tendrá la propuesta de inversión de TI sobre el perfil de riesgos del negocio (reducción o incremento del riesgo)?			X				2				X			3
89	¿Para aprobar una decisión del negocio, como la condición, el costo y las oportunidades se sopesan frente al cambio estimado a la exposición al riesgo de TI?		X					1			X				2
RG3.4	**Aceptar el riesgo de TI.**							**1**							**3**
90	¿Se utilizan umbrales de tolerancia como guía para decidir si se acepta el nivel de exposición al riesgo residual?			X				2					X		4
91	¿Se realizan evaluaciones de riesgos y se toma en consideración la información pertinente de los informes de análisis de riesgo, tales como las probabilidades de pérdida y los rangos, las opciones de respuesta al riesgo, las expectativas de costo / beneficio, y los posibles efectos de riesgos adicionales?			X				2					X		4
92	¿Se realizan análisis con los propietarios de procesos del negocio para examinar la relación riesgo/beneficio y así determinar donde gastar el presupuesto de los riesgos "conocidos" para permitir la aceptación del mismo?		X					1					X		4
93	¿Se definen acuerdos comerciales de aceptación de riesgos o, de no ser aceptables, los requisitos de respuesta a los riesgos correspondientes?		X					1					X		4
94	¿Se documenta cuando se toma una decisión de considerar un riesgo fuera de los umbrales de tolerancia justificando la decisión (p. ej.: una importante oportunidad estratégica del negocio)?	X						0		X					1

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
95	¿Las decisiones de aceptación de riesgos y los requisitos de respuesta a riesgos son comunicados a través de las líneas organizacionales según los riesgos empresariales establecidos, políticas de gobierno corporativo y procedimientos?	X						0		X					1
RG3.5	**Priorizar las actividades de respuesta a los riesgos de TI.**							**1**							**2**
96	¿Las actividades de respuesta al riesgo son evaluadas para identificar las que tienen mayor probabilidad de impacto sobre la reducción del riesgo total?		X					1				X			3
97	¿Se cuantifican los efectos esperados en relación a la frecuencia y la probable magnitud de los escenarios de riesgo a través de la aplicación planificada de controles, capacidades y recursos?		X					1				X			3
98	¿Se definen proyectos para la gestión de riesgos con énfasis en la reducción de concentración del riesgo (p. ej.: mejoras en arquitectura), implementación de controles que abarquen varios tipos de riesgos y que sean rentables, implementación de controles que mejoran la eficacia de los procesos y evitan la excesiva toma de riesgos?		X					1			X				2
99	¿Se documenta la razón fundamental de la respuesta a riesgos de TI, las limitaciones y cómo la decisión está impulsando cambios en la política, controles operativos, capacidades, los despliegues de recursos y planes de comunicación?	X						0		X					1
100	Para los casos que aplica, ¿Se documenta las causas por las cuales se excede o queda por debajo del apetito al riesgo y la tolerancia?		X					1				X			3
RE	**Evaluación del Riesgo.**							**1**							**3**
RE1	**Recopilar datos.**							**1**							**3**
RE1.1	**Establecer y mantener un modelo para recopilar datos.**							**1**							**3**
101	¿Se tiene definido un modelo para la recolección, clasificación y análisis de datos relacionados a los riesgos de TI?		X					1				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
102	¿En el proceso de recolección de datos se toman en consideración múltiples tipos de eventos (p. ej.: eventos de amenaza, vulnerabilidad o pérdida) y múltiples categorías de riesgos de TI (beneficio/valor de habilitación de tecnología, programa y ejecución de proyectos de TI, operaciones y entrega de servicios de TI)?		X					1				X			3
103	¿Durante el proceso de recolección de información se toma en consideración filtros y puntos de vista para ayudar a determinar cómo los factores de riesgos específicos pueden afectar al riesgo? (p. ej.: frecuencia, magnitud, impacto en el negocio)	X						0				X			3
104	¿El modelo de recolección de información permite apoyar la medición y evaluación de los atributos de los riesgos (como disponibilidad) a través de los dominios de riesgos de TI y proporciona información útil para establecer incentivos que permitan fomentar una cultura de concientización de riesgos?		X					1				X			3
RE1.2	**Recopilar datos sobre el entorno operativo.**							**1**							**3**
105	¿El modelo de recolección de datos toma en consideración el registro de información sobre el entorno operativo de la empresa para determinar su importancia dentro de la gestión de TI?		X					1				X			3
106	¿Para recolectar información del entorno operativo se toman en consideración fuentes dentro de la empresa, departamento legal, auditoría, de cumplimiento y la oficina del CIO?			X				2					X		4
107	¿La recolección e información toma en consideración las principales fuentes de ingresos, los sistemas externos, la responsabilidad del producto, el panorama normativo, la competencia en la industria, las nuevas tendencias en la alineación de los competidores con puntos de referencia fundamentales, la madurez relativa de los principales negocios y capacidades de TI y los problemas geopolíticos?		X					1				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
108	¿La recolección de información toma en consideración datos históricos, riesgos de TI, experiencias de colegas en la industria, bases de datos y acuerdos de la industria para divulgación de eventos comunes (p. ej.: los acuerdos del sector bancario que deben publicar información de los acontecimientos de fraude)?	X						0	X						0
RE1.3	**Recopilar datos sobre eventos de riesgo.**							**1**							**3**
109	¿La recolección de datos sobre eventos de riesgos se realiza considerando eventos que han provocado o pueden provocar impacto en la generación de beneficio/valor de TI, programas, ejecución de proyectos y servicios u operaciones de TI?		X					1				X			3
110	¿La recolección de datos sobre eventos de riesgos captura datos relevantes de temas relacionados a incidentes, problemas e investigaciones?		X					1				X			3
RE1.4	**Identificar factores de riesgo.**							**1**							**2**
111	¿Se identifican factores de riesgo analizando eventos similares para el negocio, organizando los datos y resaltando los factores que contribuyen (p. ej.: los impulsores de la frecuencia y magnitud de los eventos de riesgo)?		X					1			X				2
112	¿Se realizan análisis para determinar qué condiciones específicas existían al momento de registrarse los eventos de riesgo y cómo estas condiciones pudieron haber afectado la frecuencia y la magnitud de la pérdida?		X					1			X				2
113	¿Se identifican factores comunes que contribuyen a través de múltiples eventos?		X					1				X			3
114	¿Se realizan actividades periódicas y análisis de factores de riesgo para identificar problemas de riesgos nuevos o emergentes y, para comprender qué factores de riesgo están asociados a eventos internos o externos?		X					1			X				2
RE2	**Analizar el Riesgo.**							**1**							**3**
RE2.1	**Definir el alcance del análisis del riesgo de TI.**							**1**							**4**

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
115	¿Se define el alcance del análisis de riesgos decidiendo la amplitud y profundidad de las expectativas de los esfuerzos a realizar, tomando en consideración requisitos de decisiones estratégicas (p. ej.: nuevos productos y servicios, nuevos entornos operativos, subcontrataciones, nuevos requisitos de cumplimiento), resultados de evaluaciones empresariales de riesgo de TI, respuestas de indicadores, disparadores o eventos (nuevas o emergentes amenazas); áreas que cuentan con riesgo residual fuera de los umbrales de tolerancia y necesidades de evaluaciones de operaciones en curso?		X					1					X		4
116	¿Se cuenta con un mapa de riesgos que involucra factores relevantes de riesgo y la criticidad del negocio en el ámbito de activos/recursos y desencadenadores?		X					1					X		4
117	¿La definición del alcance del análisis de riesgos se realiza luego de considerar la criticidad del negocio, los costos de medición contra el valor esperado de la información, la reducción de la inseguridad y cualquier requerimiento regulatorio general?			X				2				X			3
RE2.2	**Estimar el riesgo de TI.**							**2**							**4**
118	¿En todo el ámbito de aplicación del análisis de riesgos de TI, se realiza una estimación de la frecuencia y magnitud probable de la pérdida o ganancia asociada a los escenarios de riesgo de TI, así como la influencia de los factores de riesgo?				X			3					X		4
119	¿Al estimar los riesgos, se realiza una estimación de la cantidad máxima de daño que puede tolerar la empresa (p. ej.: una pérdida en el peor de los casos se da cuando los factores de riesgo llegan a converger), así como la oportunidad que podría obtenerse?			X				2					X		4
120	¿Durante la estimación de riesgos, son considerados escenarios en cascada o coincidencias (p. ej.: una amenaza externa más un accidente interno)?		X					1			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
121	¿Durante la estimación de riesgos, se desarrollan las expectativas de los controles específicos, capacidad de detección y medidas de respuesta tomando como base los escenarios de riesgo más importantes?		X					1				X			3
122	¿Al estimar los riesgos, se realizan evaluaciones de los controles operativos y sus probables efectos sobre la frecuencia, magnitud y factores de riesgo aplicables?	X						0					X		4
123	¿Se realizan estimaciones de los niveles de exposición a riesgos residuales y se compara con la tolerancia aceptable al riesgo para identificar exposiciones que puedan requerir una respuesta al riesgo?			X				2					X		4
RE2.3	**Identificar las opciones de respuesta al riesgo.**							**1**							**2**
124	¿Por riesgo identificado, se evalúan las opciones de respuesta a tomar como: evitar, reducir/mitigar, transferir/compartir, aceptar o explorar/aprovechar?			X				2					X		4
125	¿Se documentan y se justifican todas las posibles respuestas al riesgo?		X					1				X			3
126	¿Se definen proyectos o programas de respuesta al riesgo considerando la tolerancia al riesgo, niveles aceptables de mitigación, costos, beneficios y responsabilidades de ejecución?		X					1			X				2
127	¿Se establecen requisitos y expectativas para controles materiales en puntos adecuados o donde se espera que se extenderán los riesgos para dar una visibilidad útil?	X						0	X						0
RE2.4	**Realizar una revisión por pares del análisis de riesgos de TI.**							**1**							**3**
128	¿El análisis de riesgos de TI es documentado en función de las necesidades del negocio?		X					1				X			3
129	¿Las herramientas de estimación para los controles son calibrados apropiadamente, previo a buscar evidencias de tal forma que no estén orientados a un resultado esperado?	X						0			X				2
130	¿El recurso que se asigna para el análisis de riesgos de TI cuenta con experiencia, capacidad y el perfil de acuerdo al alcance y complejidad de la revisión de riesgos?		X					1				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
131	¿Se evalúan los resultados de las evaluaciones de riesgos de TI, determinando si se logran los objetivos de reducción de riesgo y si el valor de la información obtenida supera los costos de la medición?		X					1				X			3
RE3	**Mantener el perfil de riesgo.**							**1**							**3**
RE3.1	**Mapear los recursos de TI para los procesos del negocio.**							**2**							**2**
132	¿Se cuenta con un mapa de recursos de TI para procesos del negocio y se mantiene actualizado?			X				2			X				2
133	¿El mapa de recursos incluye procesos de negocio, personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y subcontratistas?			X				2			X				2
134	¿Se tiene clara la dependencia de las actividades del negocio en los procesos de gestión de servicios de TI y recursos de infraestructura de TI (p. ej.: aplicaciones middleware, servidores, redes e instalaciones físicas)?				X			3				X			3
RE3.2	**Determinar la criticidad de los recursos de TI para el negocio.**							**1**							**3**
135	¿Se tiene identificados qué servicios de TI y recursos de TI son necesarios para mantener el funcionamiento de los servicios y procesos clave (críticos) del negocio?			X				2					X		4
136	¿Se realizan análisis de dependencias y vínculos débiles para determinar la criticidad del negocio de los recursos de TI, partiendo de la capa de arriba hacia abajo, a las instalaciones físicas?		X					1				X			3
137	¿Se consensua con el negocio y la dirección de TI sobre la información más valiosa de la empresa y los activos relacionados con la tecnología? (p. ej.: los utilizados para gestionar operaciones del negocio, proporcionar capacidades, generar valor, proporcionar una ventaja competitiva, proteger los datos empresariales de la rotación del personal, administrar los propósitos y las decisiones de la dirección ejecutiva)		X					1				X			3
RE3.3	**Comprender las capacidades de TI.**							**1**							**2**

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
138	¿Se cuenta con un inventario y se evalúa las capacidades de TI, las habilidades y conocimientos del personal y el resultado del desempeño de todo lo relacionado a la gestión de riesgos (p. ej.: generación de beneficio/valor de TI, programas, ejecución de proyectos y servicios u operaciones de TI)?		X					1		X					1
139	¿Se evalúa dónde la ejecución normal de los procesos puede o no proporcionar los controles adecuados y la capacidad de asumir riesgos aceptables? (p. ej.: no contar con la capacidad de ejecución de proyectos de TI en áreas técnicas específicas, pero tener una sólida gestión de programas de TI y la capacidad de contrataciones externas)		X					1				X			3
140	¿Se busca constantemente reducir la variabilidad de resultados en los procesos para mejorar la estructura de control interno, mejorar el rendimiento de TI y del negocio, y explorar/aprovechar las oportunidades?		X					1		X					1
RE3.4	**Actualizar los componentes del escenario del riesgo de TI.**							**1**							**2**
141	¿Para mantener actualizados los componentes de escenarios de riesgos de TI, se realizan evaluaciones periódicas de la colección de atributos y valores a través de escenarios de riesgos de TI y sus conexiones inherentes a las categorías de impacto en el negocio?		X					1		X					1
142	¿Se ajustan las entradas de escenarios de riesgo basadas en los cambios de las condiciones de riesgos y amenazas emergentes para generar beneficio/valor de programas, ejecución de proyectos y servicios u operaciones de TI?		X					1		X					1
143	¿Se actualizan las distribuciones y rangos basados en la criticidad de activos/recursos, información sobre el entorno operativo, datos de eventos de riesgos (p. ej.: análisis de causas y tendencias de pérdida, problemas en tiempo real y pérdida de datos), datos históricos de riesgos de TI y efectos de factores potenciales de riesgo (p. ej.: influencia en la frecuencia y/o magnitud de los escenarios de riesgo de TI y su impacto potencial en el negocio)?		X					1			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
144	¿La actualización de escenarios de riesgo incluye la vinculación de tipos de eventos (por categoría, sector de negocio y área funcional) a las categorías de riesgo y categorías de impacto en el negocio?		X					1				X			3
145	¿Se actualizan los componentes de escenarios de riesgo de TI en respuesta a cualquier cambio interno o externo considerado como significativo y es revisado periódicamente con un margen mínimo de un año?		X					1					X		4
RE3.5	**Mantener el registro de los riesgos de TI y el mapa de riesgos de TI.**							**2**							**4**
146	¿Se utilizan herramientas para mantener el perfil de riesgos así como los registros de riesgos de TI y un mapa de riesgos?			X				2					X		4
147	¿El perfil de riesgos es construido a partir de la evaluación de riesgos del negocio relacionados a TI, componentes de escenarios de riesgos, datos recopilados de eventos de riesgo, análisis de riesgos en curso y resultados de evaluaciones independientes de TI?			X				2					X		4
148	¿El proceso de mantenimiento del perfil de riesgos incluye la actualización de atributos clave como el nombre, descripción, propietario, frecuencia esperada y real, la magnitud esperada y real de escenarios de riesgos asociados, el impacto potencial y actual en el negocio, la disposición o acción ante el riesgo (p. ej.: aceptar, transferir, mitigar, evitar)?		X					1					X		4
149	¿El mantenimiento del mapa de riesgos incluye la actualización de ponderaciones para cada dimensión? (p. ej.: frecuencia, magnitud, impacto en el negocio, costo para hacer frente al riesgo de acuerdo a la tolerancia aceptable)		X					1				X			3
150	¿Se actualiza el mapa de riesgos de TI en respuesta a cualquier cambio interno o externo considerado como significativo y es revisado periódicamente con un margen mínimo de un año?			X				2					X		4
RE3.6	**Desarrollar indicadores de riesgos de TI.**							**0**							**2**
151	¿Se definen métricas o indicadores que apuntan a eventos e incidentes relacionados con TI que puedan afectar al negocio?	X						0			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
152	¿La definición de indicadores se basa en aquello que compromete la exposición y capacidad de gestión de riesgos?	X						0				X			3
153	¿Se cuenta con indicadores que alertan cuando la exposición al riesgo supera los umbrales de riesgo aceptables?	X						0			X				2
154	¿Se retroalimenta a la dirección para que comprenda la utilidad de los indicadores de riesgo, lo que son, lo que cubren, desde la infraestructura a través de una visión estratégica y qué acciones tomar si estas se disparan (p. ej.: actualizar el perfil de riesgos, ajustar las actividades de respuesta al riesgo)?	X						0				X			3
155	¿Se revisan periódicamente los KRI's utilizados por la administración, para recomendar ajustes de acuerdo a los cambios en las condiciones internas y externas?	X						0		X					1
RR	**Respuesta al Riesgo.**							**1**							**3**
RR1	**Articular el riesgo.**							**1**							**3**
RR1.1	**Comunicar los resultados del análisis del riesgo de TI.**							**1**							**3**
156	¿Se retroalimentan los resultados de análisis de riesgos en términos y formatos útiles para apoyar la toma de decisiones del negocio y, en el contexto riesgo/retorno?		X					1				X			3
157	¿La comunicación de riesgos incluye la probabilidad de pérdida y/o ganancia, rangos y niveles de confianza que permitan gestionar el balance entre riesgo/rentabilidad?			X				2					X		4
158	¿Se identifican y retroalimentan los impactos negativos de eventos y escenarios que debieran impulsar decisiones de respuesta y, los efectos positivos de eventos y escenarios que representan oportunidades que deben canalizarse para evaluar redefinir la estrategia y objetivos?		X					1			X				2
159	¿Se provee información a quienes toman decisiones para comprender los peores escenarios y los más probables, consideraciones legales y regulatorias, exposiciones de una debida diligencia y la importancia de la reputación?		X					1				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
160	¿La retroalimentación de los resultados incluye componentes claves de riesgo (p. ej.: frecuencia, magnitud, impacto), estimar la magnitud probable de pérdida o futura ganancia, calcular escenarios de estimaciones de potenciales pérdidas/ganancias (p. ej.: una frecuencia probable de tres a cinco veces por año y una probable magnitud de pérdida entre S/. 1,000.00 y S/. 5,000.00 con un 90% de confianza)?			X				2				X			3
RR1.2	**Informar las actividades de la gestión de riesgos de TI y el estado de cumplimiento.**							**1**							**2**
161	¿Se establecen necesidades de informes de resultados de gestión de riesgos de TI por las principales áreas interesadas (p. ej.: La junta, comité de riesgos, funciones de control de riesgos, unidades del negocio)?			X				2				X			3
162	¿Para presentar informes estratégicos y eficientes en materia de riesgos de TI, se aplican principios de pertinencia, eficiencia, puntualidad y precisión?	X						0			X				2
163	¿Se retroalimenta la eficacia y rendimiento de la gestión de riesgos, eficacia de los controles, rendimiento de procesos, problemas y carencias, situación actual, eventos e incidentes y el impacto en el perfil de riesgos?		X					1			X				2
RR1.3	**Interpretar resultados de evaluaciones independientes del riesgo de TI.**							**1**							**3**
164	¿Se revisan y se da seguimiento a resultados o hallazgos de terceros, auditoria interna, control de calidad, autoevaluaciones, entre otras?		X					1				X			3
165	¿Los resultados de evaluaciones independientes se mapean tomando en consideración la tolerancia establecida al riesgo?		X					1			X				2
166	¿Se toman en consideración las brechas y las exposiciones del negocio para orientar el objetivo de la gestión de riesgos o establecer necesidades de análisis de riesgos?			X				2				X			3
167	¿Se retroalimenta al negocio para que comprenda cómo los planes de acción correctiva impactan el perfil de riesgos global?		X					1				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
168	¿Se evalúan los resultados de evaluaciones independientes para identificar oportunidades para la integración con esfuerzos de corrección y otras actividades de gestión de riesgos?		X					1			X				2
RR1.4	**Identificar las oportunidades relacionadas con TI.**							**1**							**2**
169	¿En situaciones recurrentes, se consideran los niveles de riesgos de TI para procesos del negocio relacionados a la capacidad de gestión de riesgos de TI, unidades de negocio, productos, etc.?		X					1				X			3
170	¿Se evalúan áreas con riesgos relativos y capacidad equivalente de riesgo (es decir, que tienen capacidad de asumir más riesgo) para identificar oportunidades relacionadas con TI que permitan aceptar un riesgo mayor y mejorar el crecimiento y rentabilidad?	X						0		X					1
171	¿Se buscan oportunidades donde las TI permitan apalancamiento empresarial, reducción de gastos de coordinación de la empresa, aprovechar las economías de escala y alcance de ciertos recursos comunes a varias líneas de negocio, aprovechar las diferencias estructurales con competidores y coordinar actividades entre las unidades del negocio o en la cadena de valor?			X				2				X			3
RR2	**Gestionar el riesgo.**							**1**							**3**
RR2.1	**Inventario de controles.**							**1**							**3**
172	¿Se cuenta con un inventario de controles establecidos para la gestión de riesgos, los cuales se toman de acuerdo al apetito al riesgo y su tolerancia?		X					1					X		4
173	¿Los controles de riesgos se encuentran clasificados (p. ej.: predictivo, preventivo, detectivo, correctivo) y se encuentran mapeados y agrupados a riesgos específicos de TI?		X					1					X		4
174	¿Se diseñan y aplican pruebas periódicas de diseño de controles y pruebas para la eficacia operativa de controles?	X						0				X			3

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
175	¿Se analizan e identifican los procedimientos y la tecnología a utilizar para supervisar el funcionamiento de los controles (por ejemplo, el seguimiento de los controles que intervenga o la automatización de los procesos de supervisión de la empresa)?	X						0			X				2
176	¿Se cuenta con una clasificación de controles que incluya las siguientes categorías: Controles desplegados alineados a las expectativas con deficiencias operativas no conocidas, controles alineados a las expectativas con deficiencias operativas conocidas, controles que superan las expectativas con deficiencias operativas no conocidas?		X					1			X				2
RR2.2	**Monitorear la alineación operacional con los umbrales de tolerancia al riesgo.**							**1**							**4**
177	¿Las áreas del negocio aceptan la responsabilidad de operar dentro de sus niveles de tolerancia individual como del portafolio, así como de la incorporación de herramientas para supervisar los procesos operativos clave?			X				2					X		4
178	¿Se monitorea el rendimiento y eficacia del control así como la variación de los umbrales con los objetivos?		X					1				X			3
179	¿Se obtienen compromisos con la dirección sobre los indicadores que funcionaran como KRI's?	X						0				X			3
180	¿La implementación de KRI's, establece umbrales, puntos de control (p. ej.: semanal, diario, continuo) y configuración de notificaciones (p. ej.: dirección del área del negocio, alta dirección, auditoria interna) de tal forma que los implicados puedan ajustar sus planes de trabajo?	X						0					X		4
181	¿Se realizan análisis detallados para determinar las zonas de riesgos residuales fuera de los umbrales de tolerancia?			X				2					X		4
RR2.3	**Responder a la exposición y oportunidad de los riesgos identificados.**							**1**							**3**

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
182	¿Se hace hincapié en los proyectos para los cuales se espera reducir la frecuencia y magnitud de eventos adversos y pérdidas equilibrando con proyectos que permitan el aprovechamiento de oportunidades estratégicas de negocio?		X					1				X			3
183	¿Se fomentan discusiones de análisis de costo/beneficio respecto a la contribución de controles nuevos o existentes que operan dentro de los umbrales de tolerancia al riesgo de TI?	X						0		X					1
184	¿Se seleccionan controles de TI basados en amenazas específicas, el grado de exposición, la pérdida probable y requisitos obligatorios especificados en estándares de TI?		X					1					X		4
185	¿Se monitorean los cambios en el perfil de riesgos operativos subyacentes al negocio y se ajusta la clasificación de respuesta a los riesgos?			X				2					X		4
RR2.4	**Implementar controles.**							**0**							**3**
186	¿Se definen los pasos a seguir para garantizar la implementación efectiva de nuevos controles y ajustes a controles existentes?	X						0				X			3
187	¿La implementación de nuevos controles de riesgo es comunicada previamente a los interesados clave?		X					1				X			3
188	¿Se realizan pruebas piloto de los controles diseñados revisando los resultados del rendimiento para garantizar el funcionamiento?	X						0			X				2
189	¿Se mapean los nuevos controles operativos y se actualizan los mecanismos de control para medir el rendimiento del control en el tiempo y dar tratamiento inmediato con acciones correctivas cuando sea necesario?		X					1				X			3
190	¿Se identifica y capacita al personal sobre los nuevos procedimientos de control que se han implementado?	X						0				X			3
RR2.5	**Informar el progreso del plan de acción de los riesgos de TI.**							**2**							**4**
191	¿Se monitorean los planes de acción de riesgos de TI a todos los niveles para garantizar la eficacia de las acciones necesarias y determinar si se obtuvo la aceptación del riesgo residual?			X				2					X		4

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
192	¿Se garantiza que las acciones realizadas para mitigar el riesgo de TI son propiedad del responsable del proceso afectado y que las desviaciones encontradas son reportadas a la alta dirección?			X				2					X		4
RR3	**Reaccionar ante eventos.**							**2**							**3**
RR3.1	**Mantener planes de respuesta a incidentes.**							**2**							**3**
193	¿Se documentan los planes de respuesta a amenazas por medio de documentos que describan los pasos a seguir cuando un evento de riesgo pueda causar un impacto en la estrategia del negocio (incidentes relacionados con TI) o que ya ha causado un impacto en el negocio?			X				2					X		4
194	¿Se mantiene una comunicación abierta sobre la aceptación de riesgos, actividades de gestión de riesgos, técnicas de análisis y los resultados disponibles para ayudar con la preparación del plan de respuesta a riesgos de TI?			X				2				X			3
195	¿En la definición de planes de respuesta a incidentes de riesgos de TI, se toma en consideración el tiempo que la empresa puede estar expuesta y cuánto tiempo se tardaría en recuperar si este llegara a materializarse?		X					1					X		4
196	Basados en el impacto potencial o conocido, ¿Se define cómo debe escalarse en toda la empresa para dar respuesta a un riesgo, desde la gestión del negocio hasta los comités ejecutivos?		X					1			X				2
197	¿Se valida que los planes de respuesta a incidentes en procesos críticos son los adecuados?			X				2					X		4
RR3.2	**Monitorear el riesgo de TI.**							**2**							**4**
198	¿Se monitorea el ambiente para determinar si un control se incumple para tomar acciones, ya sea si se escala al siguiente paso de acuerdo al plan de respuesta o se confirma que vuelva a los límites aceptables?		X					1				X			3
199	¿Los incidentes son clasificados (p. ej.: pérdida de negocio, error del sistema, fraude, demanda) y se compara la exposición real contra los umbrales de tolerancia?			X				2					X		4

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
200	¿Se comunican los impactos comerciales de incidentes a quienes toman decisiones?				X			3					X		4
201	¿Se supervisa que la política de riesgos se cumpla y que exista una claridad en las responsabilidades para las acciones de seguimiento?				X			3					X		4
RR3.3	**Iniciar respuesta a incidentes.**							**1**							**3**
202	¿Se definen planes de acción para minimizar el impacto de un incidente en curso?			X				2					X		4
203	¿Al detectar un incidente, se identifica la categoría para cumplir con los pasos definidos en el plan de respuesta y, se comunica a las partes interesadas y afectadas de la ocurrencia del mismo?		X					1				X			3
204	¿Se analiza el incidente y se identifica el tiempo necesario para llevar a cabo el plan de respuesta haciendo los ajustes según corresponda a la situación en curso, asegurando que se adopta la medida correcta?		X					1			X				2
RR3.4	**Comunicar las lecciones aprendidas de los eventos de riesgo.**							**1**							**3**
205	¿Se evalúan los eventos adversos anteriores, pérdidas y oportunidades de pérdida para determinar si hubo una falla derivada de la falta de consciencia, capacidad o motivación?		X					1			X				2
206	¿Se buscan causas raíz de los eventos de riesgo similares y se evalúa la eficacia de las acciones tomadas antes y ahora para determinar comportamientos y el alcance de problemas subyacentes (p. ej.: problemas sistemáticos graves contra un caso aislado que podría ser gestionado a través de la capacitación del personal o proveer mayor documentación de procedimientos)?		X					1			X				2

Continúa…

CRITERIO DE EVALUACIÓN		ANTES							DESPUÉS						
		FRECUENCIA						SCORE	FRECUENCIA						SCORE
		0	1	2	3	4	5		0	1	2	3	4	5	
207	¿Se buscan soluciones tácticas, posibles inversiones en proyectos, o ajustes en el gobierno del riesgo global, a través de la evaluación y/o a través de los procesos de respuesta para mitigar el riesgo en las operaciones de TI y los incidentes de prestación de servicios relacionados con la oferta y niveles de servicios de TI (p. ej.: defectos, reproceso), la integración con la oficina de servicios de TI, el proceso de respuesta a incidentes y el proceso de gestión de problemas de TI; con el objetivo de identificar y corregir la causa subyacente?		X					1				X			3
208	¿Se comunica la causa raíz del problema, los beneficios, los incidentes en los programas de TI y en la ejecución de proyectos por medio de una comunicación abierta a través de las funciones del negocio y TI?		X					1				X			3
209	¿Se comunica la causa raíz, los requisitos adicionales de respuesta al riesgo y las mejoras en los procesos de riesgo para los procesos de gobierno y toma de decisiones?		X					1				X			3

Elaboración: Propia

Anexo 2: Matriz de Consistencia

Problema	Objetivos	Hipótesis	Variables	Indicadores	Dimensiones	Técnicas	Instrumento	Metodología
Problema General:	**Objetivo General:**		**Dependiente:**					**Tipo y Diseño:**
¿Cuál es el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?	Describir el nivel de madurez de la aplicación del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.	Sin Hipótesis	Gestión de Riesgos de Tecnología de Información	Gobierno del Riesgo.	- Visión común de riesgo. - Integración con el ERM. - Conciencia de los riesgos del negocio.	- Encuesta. - Observación.	- Modelo de Madurez del Gobierno de Riesgo. - Guía de Observación.	Tipo de Investigación: No Experimental. Diseño de Investigación: Descriptivo
Problema Específico:	**Objetivo Específico:**							**Población:**
a. ¿Cuál es el nivel de madurez del dominio "Gobierno del Riesgo" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?	a. Analizar el nivel de madurez del dominio "Gobierno del Riesgo" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.	Sin Hipótesis						Personal que labora en la Caja Rural de Ahorro y Crédito "Los Andes" S.A. (522 personas)
b. ¿Cuál es el nivel de madurez del dominio "Evaluación de Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?	b. Analizar el nivel de madurez del dominio "Evaluación de Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.	Sin Hipótesis		Evaluación de Riesgos.	- Recolección de datos. - Análisis de riesgos de TI. - Mantenimiento del perfil de riesgo.	- Encuesta. - Observación.	- Modelo de Madurez de la Evaluación de Riesgos. - Guía de Observación.	
c. ¿Cuál es el nivel de madurez del dominio "Respuesta a los Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015?	c. Analizar el nivel de madurez del dominio "Respuesta a los Riesgos" del Marco de Trabajo RISK IT en la Gestión de Riesgos de Tecnología de Información en la Caja Rural de Ahorro y Crédito Los Andes en el periodo Diciembre 2014 a Diciembre 2015.	Sin Hipótesis		Respuesta a los Riesgos.	- Articulación del riesgo. - Gestión del riesgo. - Reacción a los eventos.	- Encuesta. - Observación.	- Modelo de Madurez de Respuesta a los Riesgos. - Guía de Observación.	

Elaboración: Propia