UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

MODELO DE GESTIÓN DE RIESGOS DE TI PARA DAR SOPORTE A LOS PROCESOS COMERCIALES DE LAS EMPRESAS DISTRIBUIDORAS DE MATERIALES DE CONSTRUCCIÓN EN LA REGIÓN LAMBAYEQUE

TESIS PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR
DANTE LUIS ORDINOLA DEL CASTILLO

ASESOR
RICARDO DAVID IMAN ESPINOZA
https://orcid.org/0000-0003-0409-8773

Chiclayo, 2021

MODELO DE GESTIÓN DE RIESGOS DE TI PARA DAR SOPORTE A LOS PROCESOS COMERCIALES DE LAS EMPRESAS DISTRIBUIDORAS DE MATERIALES DE CONSTRUCCIÓN EN LA REGIÓN LAMBAYEQUE

PRESENTADA POR:

DANTE LUIS ORDINOLA DEL CASTILLO

A la Escuela de Posgrado de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADO POR:

Gregorio Manuel León Tenorio

PRESIDENTE

María Ysabel Arangurí García

SECRETARIO

Ricardo David Iman Espinoza

VOCAL

Dedicatoria

A Dios quien ha sido mi guía, fortaleza y su bendición a diario han estado conmigo hasta el día de hoy.

A mis padres por su apoyo incondicional y haberme forjado como la persona que soy, motivando constantemente para alcanzar mis logros.

A mi esposa por su paciencia, comprensión y amor, permitiendo dar el máximo de mí, siempre estaré agradecido.

Epígrafe

"He aprendido que el mundo quiere vivir en la cima de la montaña, sin saber que la verdadera felicidad está en la forma de subir la escarpada"

Gabriel García Márquez

Agradecimientos

A mi asesor Mtro. Ricardo David Imán Espinoza y la Mtro. María Ysabel Arangurí García, por el apoyo brindado durante el desarrollo de la tesis, brindando sus recomendaciones basadas en su experiencia profesional.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

Resumen

La presente investigación centra su estudio en la necesidad de incluir la gestión de riesgos de tecnologías de la información (TI) en empresas distribuidoras de materiales de construcción de la región Lambayeque, según un diagnóstico realizado a una muestra de cuatro empresas, se detectó que no tienen implementado una metodología de gestión de riesgos efectiva que ayude a dar soporte a los procesos comerciales, evitando su paralización de dichos procesos, denigrar la imagen institucional y generar pérdidas económicas para la organización.

El objetivo general formulado para la investigación es desarrollar un modelo de gestión de riesgos de TI para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque.

El modelo propuesto ha sido validado a través del juicio de expertos midiendo su confiabilidad utilizando el alfa de Cronbach y la concordancia de la evaluación de expertos con base en Kendall. Así mismo se aplicó en una empresa distribuidora de materiales de construcción de la región Lambayeque como estudio de caso. Se identificaron escenarios de riesgo, realizándose el cálculo y la clasificación del mismo, de acuerdo a los criterios de aceptación establecidos. Asimismo, se plantearon planes de tratamiento para mitigar los riesgos con un nivel no aceptable para la organización.

Palabras Clave: Gestión de riesgos de TI, procesos comerciales, empresas distribuidoras de materiales de construcción.

Abstract

This research focuses its study on the need to include information technology (IT) risk management in construction materials distribution companies in the Lambayeque region, according to a diagnosis carried out on a sample of four companies, it was detected that no have implemented an effective risk management methodology that helps to support business processes, avoiding their paralysis of these processes, denigrating the institutional image and generating economic losses for the organization.

The general objective formulated for the research is to develop an IT risk management model to support the business processes of the construction materials distribution companies in the Lambayeque region.

The proposed model has been validated through expert judgment, measuring its reliability using Cronbach's alpha and the agreement of the expert evaluation based on Kendall. Likewise, it was applied in a construction materials distribution company in the Lambayeque region as a case study. Risk scenarios were identified, calculating and classifying it, according to the established acceptance criteria. Likewise, treatment plans were proposed to mitigate risks with a level not acceptable to the organization.

Keywords: IT risk management, business processes, construction materials distribution companies.

INTRODUCCIÓN

En el presente trabajo de investigación se propuso un modelo de gestión de riesgos de TI, para dar soporte a los procesos comerciales de las empresas distribuidoras de la región Lambayeque. Cualquier incidente derivado de fuentes tecnológicas puede repercutir sobre las estrategias de una organización. Es así que, la paralización, deterioro o fallas derivadas del uso de TI podrían afectar financieramente las organizaciones, o enfrentar acciones legales, que alterarían la imagen corporativa, conllevando a repercutir las operaciones a nivel operativo y estratégico [1].

En el contexto internacional, el servicio de mensajería instantánea llamado Whatsapp [2], informó sobre un inconveniente en su conexión a nivel mundial, dejando sin comunicación por un tiempo aproximado de 2 horas a un millón de usuarios, repercutiendo sobre la imagen corporativa de la organización. “Supply Chain Resilience” del Business Continuity Institute en su reporte manifestó que las interrupciones del servicio que no se encuentran planeadas tienen como importantes efectos en la productividad en un 68% y el incremento del costo laboral

en un 53% dentro de la organización [3]. La aerolínea comercial estadounidense Delta Airlines, en agosto del 2016, presentó problemas debido a la caída en su sistema informático, generando retrasos y cancelaciones de vuelos durante varios días; esto afecto económicamente a la aerolínea lo que conllevo a compensar a todos sus pasajeros afectados obsequiando cupones y promociones para sus vuelos [4].

En el contexto nacional, el 22 de mayo del año 2014, en la ciudad de Lima, el Aeropuerto Internacional Jorge Chávez, el área de migraciones presento inconvenientes en sus operaciones debido a la caída del sistema informático, ocasionando malestar entre los pasajeros, los cuales corrían el riesgo de perder sus vuelos; este acontecimiento provocó el descontento de aproximadamente 1200 personas que abordarían el avión de aproximadamente 8100 que requieren el servicio, lo que afectó negativamente a la organización [5]. La Junta de Decanos de los Colegios de Contadores Públicos del Perú, el 23 de junio del 2019, manifestó la ocurrencia de fallas de manera reiterativa de los sistemas informáticos de la Superintendencia Nacional de Aduanas y Administración Tributaria (Sunat), sucedidos entre el 4 y 11 de junio del mismo año, el cual afectó a cerca de 1 millón de empresas y cerca de 150 mil contadores públicos en la realización de sus declaraciones de impuestos. Asimismo, dicha institución, solicitó al Gobierno Nacional, que convoque una auditoría informática internacional, para que puedan determinar la causa que produce el mal funcionamiento de los sistemas de la Sunat y poder identificar a los responsables de la institución [6]. La institución financiera Interbank Perú, entre el 11 y 16 de diciembre del 2015, sufrió una caída en su sistema informático, afectando a los consumidores que no pudieron disponer de sus fondos que existían en sus cuentas, así como de los diversos servicios o productos contratados. Como resultado de este incidente, INDECOPI, multó a dicha entidad financiera por un importe de S/ 76,950.00 nuevos soles, por afectar a su cartera de clientes [7].

En el contexto regional, la empresa de telecomunicaciones Movistar, el 19 de junio 2020 [8], registró un incendio de regular intensidad dentro sus instalaciones, ubicada en la ciudad de Chiclayo, región de Lambayeque, en la calle Elías Aguirre cuadra 8, causando la afectación de sus servicios como telefonía móvil y fija; TV Paga e internet fijo, miles de usuarios quedaron incomunicados por más de 12 horas en algunas zonas de la región Lambayeque.

En cuanto a las empresas distribuidoras de materiales de construcción de la región Lambayeque, continuamente han sufrido incidentes por daños en la infraestructura de red, imposibilidad de acceso a la información como consecuencia de la infección y propagación de virus informáticos, los mismos que afectaron la continuidad de los procesos. Esto se manifiesta en la falta de conocimiento de la gestión de riesgos. En 2018, Empresa 1, sufrió la caída de su sistema informático interno, debido a la infección de un virus Ransomware, el cual afectó todas las áreas de la empresa; las operaciones se paralizaron por dos días, hasta restablecer los servicios y la información, afectando a los clientes y causando pérdidas económicas para la empresa. En el 2019 en la Empresa 2, el área de servidores sufrió un incendio debido a un corto circuito, destruyendo todo el equipamiento tecnológico lo que ocasionó la pérdida de información histórica para la empresa, ya que no contaban con mecanismos de respaldo de información. En este mismo año la Empresa 3, el área de cobranzas se vio afectado en sus operaciones debido a que el sistema web no se encontraba disponible por una interrupción del acceso a la red de internet. El proveedor de internet tardó cuatro días en subsanar el problema. La empresa no contaba con un respaldo de otro proveedor de internet, esto ocasiono paralizar todas las operaciones del área de cobranzas.

Estos eventos demuestran la importancia de una adecuada gestión de los riesgos de TI, que perjudican el logro de la estrategia organizacional y los objetivos operativos.

En base a la realidad problemática descrita en el apartado anterior, se formuló la siguiente pregunta ¿De qué manera se puede dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción, de la región Lambayeque?. Para dar respuesta a la interrogante se propuso que, con la implementación del modelo de gestión de riesgos de TI se da soporte a los procesos comerciales de empresas distribuidoras de materiales de construcción de la región Lambayeque.

El objetivo general de esta investigación es, desarrollar un modelo de gestión de riesgos de TI para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque. Para lograr el cumplimiento de este objetivo se ha planteado los siguientes objetivos específicos: identificar las metodologías, estándares y normas vigentes de gestión de riesgos de TI, que permitan alinear un modelo de gestión de riesgos adaptado a los procesos comerciales de las empresas distribuidoras de materiales de construcción; proponer un modelo de gestión de riesgos de TI adaptado, para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque; validar el modelo de gestión de riesgos de TI, mediante juicio de expertos y validar la utilidad del modelo propuesto para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción.

Esta investigación se justifica en el aspecto social, debido a que el personal de las organizaciones deben ser conscientes del valor que proporciona la adecuada supervisión de riesgos de TI, generando la sensibilización acerca de la eficacia con que se tratan los riesgos de manera planificada; de esta manera se tuvo la certeza razonable de entender el grado en que la entidad está alcanzando los objetivos estratégicos y operacionales, impactando positivamente en el clima organizacional y creando una correcta imagen empresarial. Tambien se justifica esta investigación desde el punto de vista económico, en el que resulta importante resaltar que un adecuado y correcto manejo de riesgos de TI, logra incrementar el nivel de

productividad de los procesos comerciales debido a la identificación oportuna de los riesgos ante un incidente. Del mismo modo la gestión de riesgos de TI, permite establecer acciones de vigilancia permanente sobre el correcto funcionamiento de los activos y los procesos críticos que se desarrollan en las actividades, haciendo posible que la organización desarrolle con normalidad sus actividades, minimizando las pérdidas económicas. Además se considera una justificación en el aspecto tecnológico, porque se desarrolló una guía para gestionar los riesgos de TI sustentado en normas y métodos que permitió adoptar mecanismos de respuestas rápidas ante los incidentes, logrando minimizar el grado de vulnerabilidad de los activos tecnológicos de la organización; estableciéndose pautas en la capacidad de recuperación dando soporte a sus procesos comerciales.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes del problema

Para dar sustento a la propuesta presentada, se ha considerado fundamentar a través de los antecedentes seleccionados como investigaciones previas relacionadas con el tema.

En 2015, Murillo y Rivas [9], en su investigación realiza un análisis sobre el riesgo que han presentado las microempresas comercializadoras frente a las empresas multinacionales, para lo cual propone un modelo establecido en los modelos ISO 31000:2011 y OHSAS 18001:2007 que le permita establecer acciones preventivas y correctivas para gestionar sus riesgos internos y externos y así pueda obtener una mayor rentabilidad y la sostenibilidad del negocio en el mercado nacional.

Como respuesta a la utilización de este modelo, se logró establecer una metodología para la gestión de riesgos que permitió priorizar la implementación de controles para los riesgos presentados en las microempresas comercializadoras de electrodomésticos.

Este antecedente, fue una referencia para la presente investigación en la medida que permite adaptar una metodología de gestión de riesgos para una empresa comercializadora en la que se utiliza la metodología ISO 31000:2011, siendo de gran utilidad con la propuesta que se presenta, puesto que se pretende adaptar una metodología para la empresa del sector comercial.

En 2019, José Banda [10], en su investigación detalla la realidad problemática como incidentes constantes que comprometen la seguridad de los activos de información en las empresas del sector agroindustrial de la región Lambayeque, por lo cual propone un modelo basado en ISO 31000:2018 para contribuir en la mejora de la seguridad de los activos de información, estableciendo para ello, tratamientos adecuados y efectivos que permita mitigar los riesgos a los cuales se enfrentan las empresas del sector agroindustrial.

Como resultado de esta propuesta, el modelo de gestión de riesgos de TI permitió definir métricas para monitorizar los escenarios de riesgo que afectan la seguridad de los activos de información en el sector agroindustrial, fueron identificados 20 escenarios de riesgo, de los cuales 13 eran Inaceptables y 4 tolerables, para lo cual se propusieron 8 proyectos que permitieron disminuir e nivel de riesgo.

Este antecedente, fue una referencia para la presente investigación, ya que con la utilización de metodologías y estándares pudo definir proceso para la gestión de riesgos en un sector en específico, tal y como se realizará en la presente investigación.

En 2019, Oscar Ñañez [11], en su investigación describe la necesidad de una metodología que permita realizar la identificación, evaluación y tratamiento de los riesgos de TI, que impactan negativamente en la universidad. Por ello, el autor propone un modelo basado en la norma ISO/IEC 27005 y metodología Magerit, que le ha permitido identificar en cada activo de TI, sus amenazas y vulnerabilidades,

permitiendole elaborar estrategias eficientes para el tratamientos de los riesgos en los procesos academicos y administrativos de la universidad.

Con la aplicación de este modelo en donde se evaluaron los riesgos encontrados, en base a indicadores de riesgo clave, se pudo evidenciar una mejoría en la gestión de los riesgos, identificando las brechas de seguridad y permitiendo disminuir estas brechas.

Este antecedente, fue relevante para la presente investigación, dado que realizó la evaluación y tratamiento de estos riesgos por cada activo de TI que debía protegerse, como respuesta a las activiades que realiza la OGTI, lo cual resulta importante para esta investigación en el que el Area de Tecnologías de Información carece de un plan de gestión de riesgos.

En 2018, Roberto Santa Cruz [12], en su investigación describe las brechas de seguridad existentes en el sector microfinacniero de la ciudad de Chiclayo, Perú, en donde detalla la obligatoriedad de estas empresas a establecer pautas minimas para identificar y administrar los riesgos relacionados a las tecnologías de la información en cumplimiento de lo dispuesto por la SBS.

Para el desarrollo de la propuesta, se contempla la gestión de la continuidad de los procesos del negocio basado en un modelo de gesion de riesgos de tecnologías de información en cumplimiento a las exigencias de la SBS en el sector Microfinanciero, y asimismo toma como bases las normas ISO/IEC 27001,la ISO/IEC 17799 y la metodología MAGERIT.

De la matriz de riesgos obtenida, se pudo disponer de los registros de los principales activos de TI, para implementar medidas de control y proteger los procesos de posibles amenazas y vulnerabilidades.

Este modelo propuesto para el sector microfinanciero, resalta la importancia de gestionar adecuadamente los riesgos de TI, y muestra un enfoque interesante en

el que combina la gestion de riesgos de TI y las normas que se aplican para este sector.

En 2018, Caballero y Kuna [13], utilizan las metodologías SEI CRM y Magerit v3 para realizar análisis de riesgo y gestión de proyectos de software para proponer un esquema ágil y de poco costo que permita ser realizado por diferentes organizaciones con menor recurso financiero.

Este antecedente se utiliza como referencia en esta investigación, para comprender cómo utilizar el método SEI CRM para implementar procesos de gestión de riesgos para empresas con presupuestos más bajos.

En 2019, Miguel Huaura [14], expone como problema principal la falta de gestión de riesgos en las empresas del Sector Telecomunicaciones en Perú, en donde rescata que las leyes sobre las cuales esta sujeto este sector son de cumplimiento obligatorio y que el control de riesgos de las tecnologías de información son un factor clave en la toma de decisiones.

Por ello, el autor propone el uso de la NTP ISO/IEC 31000, como soporte normativo que influye en este sector para el control de riesgos de la seguridad de la información.

La aplicación de esta norma le ha permitido identificar los posibles riesgos de pérdida de información logrando analizar de manera coherente los riesgos, facilitando indicadores y métricas de gestión como apoyo en la toma de decisiones de la alta dirección generando retroalimentación, fortalecimiento y aprendizaje a toda la empresa y mejora la confianza de todos los involucrados.

Este antecedente es relevante para la investigación, dado que, el autor destaca la correcta gestión de riesgos de seguridad de la información, lo que es de gran utilidad para esta investigación, ya que uno de los resultados que se busca es

impactar en el cumplimiento de los objetivos específicos de la organización, además al mejorar la toma de decisiones de la Alta Dirección.

En 2019, Judith Navarro [15], describe el estado situacion del área de Base de Datos y Sistemas Operativos de la Dirección General de Ingresos en Nicaragua, en donde describe que el tratamiento de los riesgos se realiza de forma empírica ocasionando que la mayoría de los casos de riesgos se materialicen.

Por ello, propone el uso de Norma ISO/IEC 27005 como alternativa de solución, el cual le permitirá gestionar los riesgos que pongan en peligro la información, lo que les permitirá reducir el impacto de los riesgos a nivel físico, lógico y organizacional.

Con la aplicación de esta norma, se desarrolló un plan para el tratamiento del riesgo, plasmado en una política de seguridad y un plan a ejecutarse, los mismos que permitiran aplicar medidas preventivas y correctivas, reduciendo los niveles de riesgo que existen como parte de la mejora de procesos dentro de la entidad.

Este antecedente fue relevante para el presente proyecto de investigación, por cómo se propone el plan para el tratamiento de la gestión de riesgos, basado en una norma, en el área de tecnologías de información.

En 2017, Eduardo Bernal [16], realiza realiza un análisis sobre las vulnerabilidades que existen en la seguridad de datos y la inexistente prevención de estos riesgos tecnológicos que se dan en los departamentos de tecnologia del sector educativo en Cuenca, Ecuador, asi como tambien da a conocer la importancia de la gestión ética sobre el personal que forma parte de los departamentos de tecnologías.

Para ello, se ha centrado en aplicar la metodología MAGERIT v3, junto a la herramienta PILAR 2017 para aplicar la norma ISO 31000:2011, que le ha permitido determinar que activos tienen mayor vulnerablidad y el impacto que ocasionaría su posible ausencia en la organización.

De la aplicación de estos estándares , le permitió crear un plan de gestión de riesgos y de gestión ética, en donde evaluó los riesgos de mayor criticidad utilizando una matriz de riesgos y que le permitió presentar un plan de contingencia de uno de los riesgos encontrados.

Con respecto a este antecedente, nos detalla su plan de gestión de riesgos y la matriz creada, algo que es importante para esta investigación puesto que se pretende utilizar una matriz de riesgos para la evaluar el nivel de criticidad de cada uno de los activos.

En 2016, Edwin Chillogallo y Victor Zambrano [17], detalla de forma breve como la Fiscalia General del Estado, evalúa, gestiona y aplica soluciones para los riesgos informáticos que actualmente se presentan.

En ese contexto, y para el desarrollo de la propuesta, el autor ha formulado una encuesta para conocer el estado actual de la gestión de riesgos, en donde pudo determinar el bajo nivel de cumplimento con respecto a la gestión de riesgos. Esto debido a la misma desorganización al momento de tomar decisiones para dar solución al problema presentado.

Por ello, el autor propone como alternativa de solución la NTE INEN-ISO 31000 y el marco de referencia MAGERIT, en donde tuvieron como factor de inclusión solo a los activos que presentaron un riesgo alto.

En respuesta a la aplicación del modelo propuesto, logró que el 100% mejorará en la aplicabilidad de la metodología, dado que se realizó un seguimiento contínuo.

Este antecendente es relevante para la presente investigación, dado que si bien la aplicación del modelo propuesto sólo se centró en los activos con mayor impacto de riesgo en la organización, queda demostrado que la aplicabilidad de este tipo de modelos propuestos debe ir siempre con al acompañamiento de uno o mas responsables que fomenten el uso de la misma y garanticen la continuidad adecuada

sobre la gestión de los riesgos, algo que es importante para esta investigación para concientizar a todos los involucrados en el proceso de gestión de riesgos de TI.

1.2. Marco teórico conceptual

1.2.1. Riesgo

Según la ISO 31000:2018 define riesgo como "el efecto de la incetidumbre sobre los objetivos".

De acuerdo a la definición anterior se puede concluir que el riesgo es un evento o circustancia que ocurre en un lugar determinado durante un período de tiempo con consecuencias positivas o negativas que pueden afectar el logro de una meta.

1.2.2. Gestión del Riesgo

Según la ISO 31000:2018 define como "actividades coordinadas para dirigir y controlar la organización con relación al riesgo".

Se concluye que la gestión de riesgos incluye las actividades de identificación, evaluación, tratamiento y control de los riesgos para que permanezcan dentro de los límites establecidos por la organización.

1.2.3. Gestión de Riesgos de Tecnologías de Información

El riesgo de las tecnologías de información surge en cualquier nivel dentro de una empresa, es ahí donde poder gestionarla implica entender el papel primordial que cumplen. La gestión como tal, es un proceso cíclico que comienza desde un conjunto de información tomada de diversas fuentes (necesidades, persona, proceso de desarrollo, presupuestos, posibilidades).

Este proceso toma esos datos, para analizarlos, realizar un listado de prioridades para establecer expectativas claras y la dirección a tomar dando como

resultado un conjunto de riesgos priorizados, los cuales van a permitir conocer la mejor estrategia a tomar.

- Análisis del riesgo

  Este es un proceso sistemático que puede estimar cual es la posibilidad que ocurra y las posibles consecuencias del efecto de cada factor de riesgo encontrado.

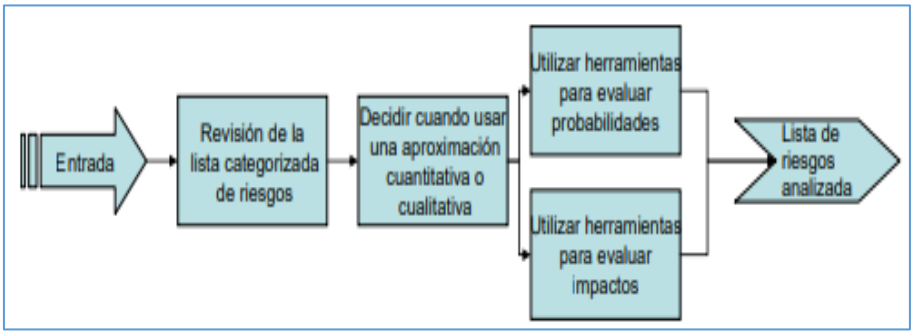


Figura 1: Proceso de Análisis de Riesgos

- Priorizar

  En la priorización se decide cuáles de los riesgos deben ser afrontados, tomando en consideración que el tiempo que se brinda es insuficiente y que los recursos son escasos para afrontar este tipo de situaciones. [18]

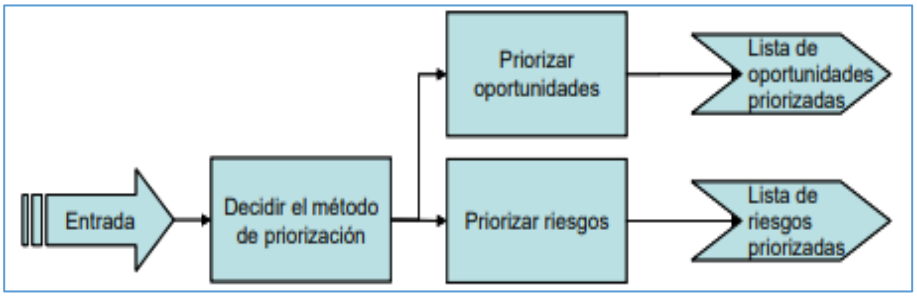


Figura 2: Proceso de Priorización

1.2.4. Estándares de Gestión de Riesgos de Tecnologías de la Información

- **ISO 31000:2018**

  Esta norma facilita pautas para poder gestionar el riesgo que se presentan en las organizaciones. La aplicabilidad de estas pautas es factible de adecuarse a cualquier organización y el contexto.

  La norma ISO31000:2018, está estructurada de la siguiente manera:

  - **Principios**

    Estos principios brindan la orientación sobre las particularidades que necesita tener para gestionar los riesgos eficientemente.

    Los principios que se describen para la gestión de riesgos se detallan de la siguiente manera:

    a) Estar integrada con los procesos de la organización.

    b) Estructurada y exhaustiva.

    c) Que se adapte a las circunstancias.

    d) Deber ser inclusiva.

    e) Debe ser dinámica.

    f) Mejor información que se dispone.

    g) Valorar factores humanos y culturales.

    h) Facilitar el proceso constante de mejora continua.

Figura 3: Principios

- **Marco de Referencia**

El propósito es acompañar a la entidad en la integración de la gestión del riesgo en sus actividades y situaciones significativas.

Este desarrollo involucra que se pueda aplicar la integración, el diseño, la implementación, valorar y mejorar la gestión del riesgo en una entidad.

Figura 4: Marco de Referencia

- **Proceso**

Es la aplicación consecuente de políticas, procedimientos y prácticas a las acciones de comunicación y consulta, determinación del contexto y evaluación del riesgo, tratamiento, para su posterior seguimiento y revisión llevando un registro e informe del riesgo.

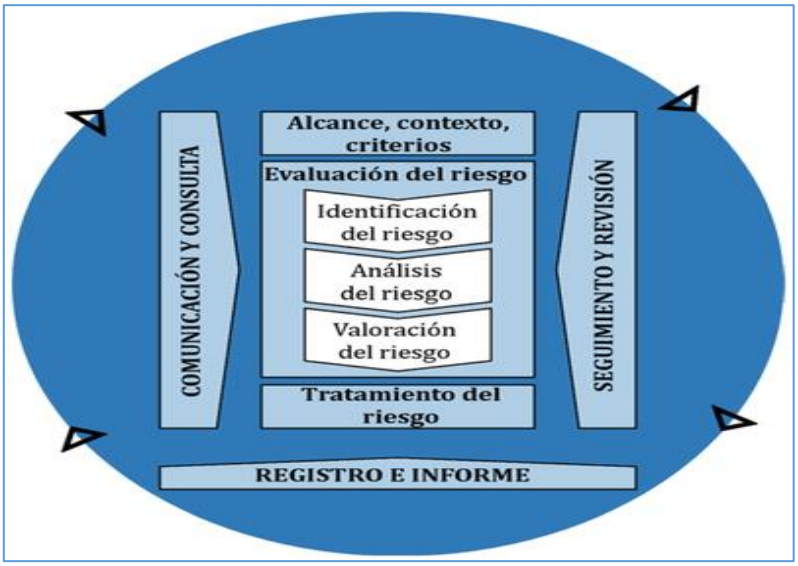


Figura 5: Proceso de Gestión del Riesgo

La evaluación del riesgo es el proceso central para la identificación, el análisis y la valoración del riesgo los mismos que se detallan a continuación:

- **Identificación del riesgo**

  Es descubrir, reconocer y detallar los riesgos que pueden apoyar o impiden a una entidad que alcance sus metas.

- **Análisis del riesgo**

  Es entender la naturaleza del riesgo y sus particularidades y de ser apropiado, el nivel del riesgo que se tiene.

- **Valoración del riesgo**

  Es realizar una comparación entre los resultados del análisis del riesgo con los criterios del riesgo que se establezcan para establecer en que momento es preciso una acción adicional.

Tratamiento del riesgo

El tratamiento del riesgo es seleccionar y aplicar las medidas más adecuadas que permitan abordar el riesgo. [19]

- **ISO 27005**

Es una norma Internacional que contiene pautas para la gestión del riesgo de seguridad de la información en una organización; se encuentra diseñada para dar soporte al aplicar un sistema de gestión de seguridad de la información (SGSI) según la norma ISO/IEC 27001. [20]

El propósito de cualquier análisis de riesgos es determinar la frecuencia con que determinados eventos puedan ocurrir y el impacto que podría causar a la organización. [21]

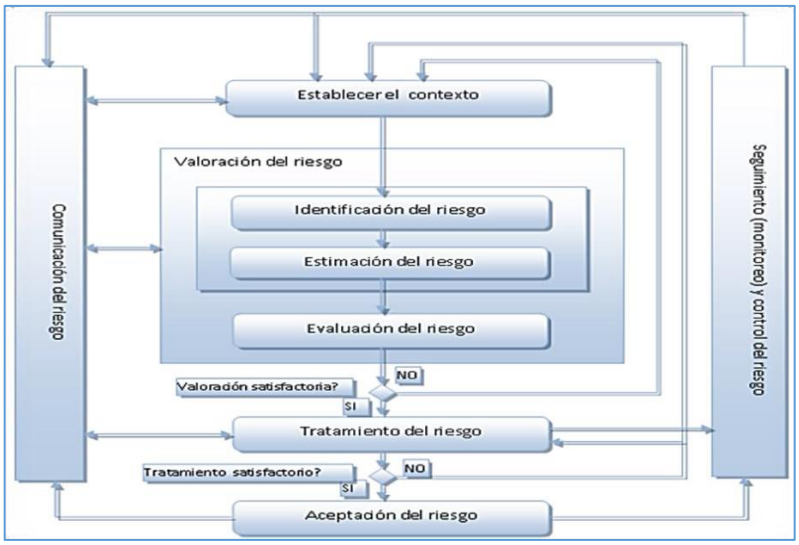


Figura 6: Proceso de Gestión de Riesgos de Seguridad de la Información

1.2.5. Metodologías de la Gestión de Riesgos de Tecnologías de la Información

- **COBIT 5**

COBIT (Control Objectives for Information and related Technology), es un marco de trabajo, y se centra en el control y supervisión de los objetivos de las tecnologías de la información (TI) desde una perspectiva de negocio.

Para COBIT 5, el Objetivo de Gobierno es la creación de valor, centrándose en la realización de beneficios, la optimización del riesgo, y la optimización de recursos. [22]

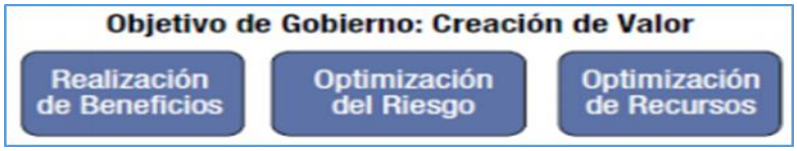


Figura 7: Objetivo de Gobierno

Asimismo, para un contexto de riesgos se presentan dos perspectivas en el uso de COBIT: la función de riesgo y la gestión de riesgos. [23]

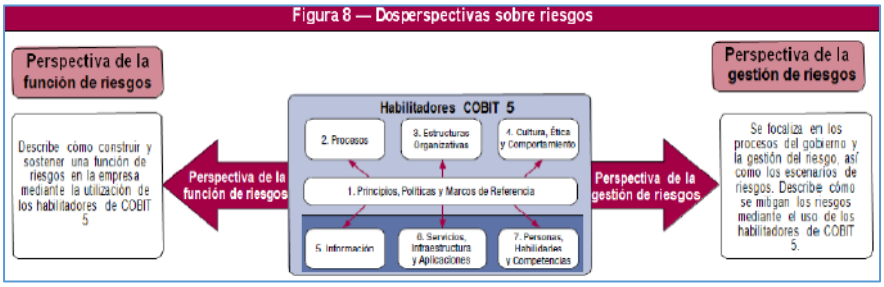


Figura 8: Dos perspectivas sobre riesgos

Principios de COBIT 5 para la gestión de riesgos:

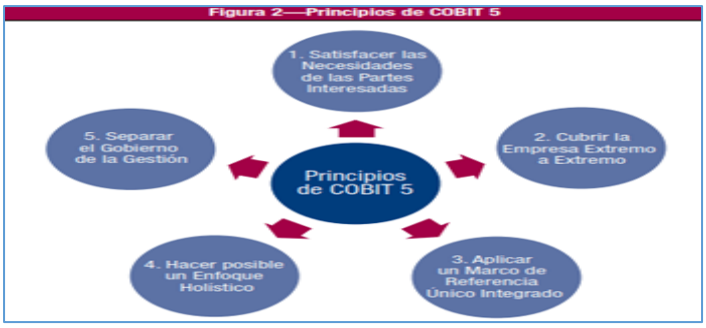


Figura 9: Principios de COBIT 5

Se tienen 02 procesos principales:

Figura 33—Procesos principales del riesgo

Procesos COBIT 5	Razonamiento
EDM03 Asegurar la optimización del riesgo	Este proceso abarca el entendimiento, la articulación y la comunicación del apetito y tolerancia al riesgo de la empresa, y asegura la identificación y gestión del riesgo asociado al valor de la empresa que está relacionado con el uso de TI y su impacto. Las metas de este proceso son: • Definir y comunicar los umbrales de riesgo y asegurar que se conozcan los riesgos clave relacionados con TI. • Gestionar de una manera efectiva y eficiente a los riesgos críticos de la empresa relacionados con TI. • Asegurar que los riesgos de la empresa relacionados con TI no excedan su apetito de riesgo.
APO12 Gestionar el riesgo	Este proceso abarca la continua identificación, evaluación y reducción del riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa. La gestión de riesgos de la empresa relacionado con TI debería ser integrada al ERM global. Se deberían balancear los costos y beneficios de gestionar el riesgo de la empresa relacionado con TI mediante: • La recolección de datos apropiados asociados al análisis de riesgos. • Manteniendo el perfil de riesgo de la empresa y articulando los riesgos. • Definiendo el portafolio de acciones de la gestión de riesgos y respondiendo al riesgo

Figura 10: Procesos principales del riesgo

- **MAGERIT**

MAGERIT permite realizar la implementación del Proceso de Gestión de Riesgos mediante un marco de trabajo, para que los órganos de gobierno tomen decisiones aplicando medidas de seguridad que generen confianza con la finalidad de minimizar ciertos riesgos.

Figura 11: MAGERIT - Marco de trabajo

Objetivos:

- **Directos**

  - Concientiza a los encargados de las tecnologías de información sobre la presencia de riesgos y la disposición de administrarlos oportunamente.

  - Ayuda a encontrar y planear el método adecuado a aplicar que permita custodiar los riesgos y ser controlados.

- **Indirectos**

  - Acondiciona a la entidad para llevar a cabo eventos de valoración, revisión y acreditación, donde se requiera.

Asimismo, se da a conocer la semejanza de los documentos que detallan los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos:

- **Modelo de valor:** determinación del valor que tienen los activos para la organización.
- **Mapa de riesgos:** informe de amenazas posibles a la que están expuestos los activos.
- **Declaración de Aplicabilidad:** Se indica sin son apropiados para aplicar en el sistema de información bajo estudio.
- **Evaluación de salvaguardas:** validación del grado de efectividad en relación a la amenaza que afrontan.
- **Estado de Riesgo:** evaluación de los activos sobre cómo reaccionan ante lo que podría pasar y lo que se encuentra desplegado.
- **Informe de Insuficiencias:** es la relación de tareas pendientes sobre lo que se debería hacer y no se ha hecho o se encuentra mal enfocado. Muestra las vulnerabilidades del sistema y/o se encuentran débilmente protegidos.
- **Cumplimiento de Normativa:** es el cumplimiento de la legislación.
- **Plan de Seguridad:** las decisiones de tratamiento de riesgos se pueden plasmar en un Plan de Seguridad que permita satisfacer los objetivos trazados por la organización. [24]

- **RISK IT**

RISK IT brinda a las organizaciones gestionar los riesgos soportados en los valores y beneficios obtenidos mediante las iniciativas de TI.

Se toma como una guía de referencia pues toma en cuenta la relación que existe entre los riesgos de negocio y los riesgos de la tecnología para la toma de decisiones. [25]

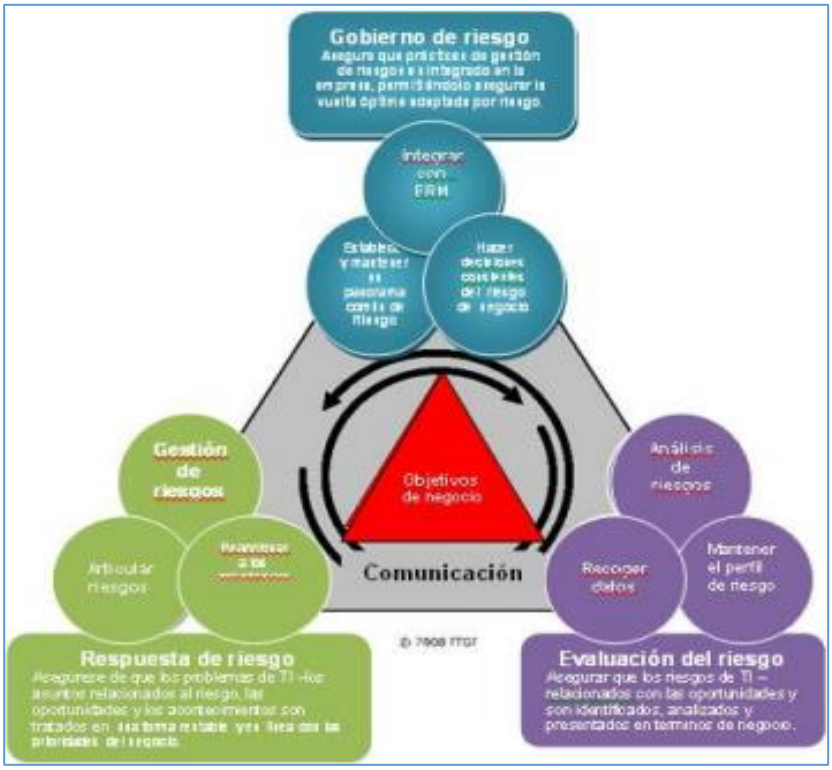


Figura 12: Marco de RISK IT

- **NIST SP 800-30**

Este método de análisis de riesgo NIST SP 800-30, define al riesgo como un impacto negativo neto de la expresión de una vulnerabilidad, considerándose tanto la probabilidad como el impacto de ocurrencia. Puede proporcionar un sustento para elaborar un esquema eficazmente para gestionar los riesgos, abarcando la identificación y evaluación de los riesgos que se encuentran en los sistemas informáticos. Su objetivo es apoyar a las organizaciones en cómo mejorar la gestión de los riesgos que se encuentran en cada uno de los procesos que TI soporta. Asimismo, brinda detalles de los controles, permitiendo la protección de los sistemas informáticos que se encargan de procesar, almacenar y transportar dicha información. [26]

Este proceso consta de cuatro pasos:

1) Elaboración.

2) Ejecución.

3) Informe de resultados.

4) Conservar la valoración.

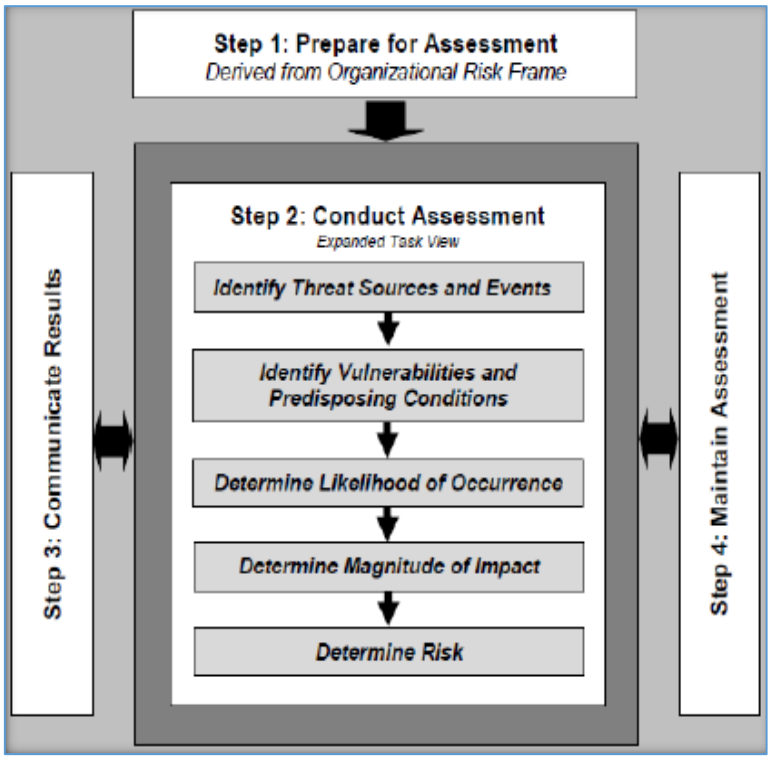


Figura 13: Procedimiento para evaluar el riesgo

- **OCTAVE**

Es una metodología de evaluación de riesgos, donde sus fases son catalogadas como las mas complicadas que las demás metodologías, fue desarrollada para ser implementada en organizaciones de más de 300 trabajadores, y se enucnetra dividaa en tres fases. La primera fase llamada Build asset-based threat profiles, detalla un perfil de cada amenaza basados en los activos,

comprende la identfiicación de bienes, amenazas prácticas actuales, vulnerabilidades y los recursos de seguridad de la organización, la segunda fase llamada Identify infrastructure vulnerabilities, identificar las vulnerabilidades de la infraestructura, se basa en componentes claves y sus vulnerabilidades técnicas, y finalmente la tercera fase llamada Develop security strategy and plans, desarrollar estrategias y planes de seguridad, con base a los riesgos, la estrategia de protección y los planes de mitigación. [27]

1.2.6. Empresas Distribuidoras de Materiales de Construcción

Son empresas encargadas de adquirir sus productos a distintos fabricantes, para luego ser comercializados y así poder distribuirlos en diversas pequeñas empresas o clientes finales, con ventas al por mayor y menor, logrando obtener ganancias y un posicionamiento en el mercado.

1.2.7. Procesos Comerciales de Empresas Distribuidoras de Materiales de Construcción

Son un conjunto de actividades que se desarrollan para cerrar una venta, involucrando diferentes áreas de la organización, los cuales inician con una estrategia comercial, el cual trata de estudiar el entorno, la competencia y las necesidades de los clientes, terminando la estrategia con el servicio ofrecido al cliente después de realizada su compra.

Elementos principales de los procesos comerciales:

- **Gestión de Compras**

  La gestión de compras es aquella que se encarga de administrar las acciones relacionadas con la logistica de una organización, es decir su funcion es planificar y controlar el inventario de productos, contactar con los proveedores y asegurar de que todas las ventas de los

productos se realicen adecuadamenta para satisfacer sus necesidades de los clientes. [28]

- **Gestión de Stock**

  Las empresas manejan grandes cantidades de mercadería las cuales deben ser monitoreadas regularmente para evitar escases o exceso y no afectar el servicio al cliente, por tanto es absolutamente imprescindible contar con un mecanismo de control de existencias para una adecuada contabilidad de stock. [29]

- **Proceso de Ventas**

  El proceso de ventas consiste en definir los pasos que una organización realiza desde el momento en que intenta llamar la atención de un potencial cliente hasta conseguir una venta efectiva de los productos o servicios de la organización, y mantener relaciones comerciales con los clientes para finalmente fidelizar al cliente [30].

CAPÍTULO II MATERIALES Y MÉTODOS

2.1. Diseño de Investigación

El tipo de estudio es cuantitavia aplicada.

Para contrastar la hipótesis se utilizó el método Pre Test – Post Test; donde se medirá la variable dependiente previa a la aplicación de la variable independiente (Pre Test), luego una medición nueva de la variable dependiente posterior a la aplicación de la variable independiente (Post Test), y finalmente aplicar la variable independiente.

Diseño de Contrastación Pre Test – Post Test:

$$G = O_1 \; X \; O_2$$

Donde:

- **G:** Grupo de estudio.
- **O1:** Dar soporte a los procesos comerciales en las empresas distribuidoras de materiales de construcción en la región Lambayeque, antes de la aplicación del modelo de gestión de riesgos de TI.

- **X:** Modelo de gestión de riesgos basado en estándares adaptados a las TI que soportan los procesos.

- **O2:** Dar soporte a los procesos comerciales en las empresas distribuidoras de materiales de construcción en la región Lambayeque, después de la aplicación del modelo de gestión de riesgos de TI.

2.2. Población, Muestra y Muestreo

En esta presente tesis se tomó como población las empresas distribuidoras de materiales de construcción las cuales on un total de 12 empresas en la región Lambayeque.

Como muestra se toma a 4 empresas distribuidoras de materiales de construcción de la región Lambayeque, las cuales son: Empresa 1, Empresa 2, Empresa 3 y Empresa 4.

Se consideró a los jefes a cargo del área de tecnologías de Información que dan soporte a los procesos comerciales de las empresas en distribuidoras de materiales de contrucción de la región Lambayeque.

En el Anexo 1, se detalla un cuadro comparativo sobre las empresas distribuidoras de ventas de materiales de construcción.

2.3. Operacionalización de Variables

Variables	Definición Conceptual	Objetivos Especifícos	Dimensiones	Indicadores	Técnica / Instrumento
Variable Independiente: Modelo de Gestión de Riesgos de TI Basados en Estándares Adaptados a las TI.	Documento orientador básico que sistematiza de manera ordenada los conceptos y metodologías de gestión de riesgos de TI.	Identificar las metodologías, estándares y normas vigentes de gestión de riesgos de TI, que permitan alinear un modelo de gestión de riesgos adaptado a los procesos comerciales de las empresas distribuidoras de materiales de construcción.	Metodologías de gestión de riesgos TI.	Número de metodologías para gestionar los riesgos de TI.	Análisis Documental
		Proponer un modelo de gestión de riesgos de TI adaptado, para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque.	Modelo de gestión de riesgos de TI.	Propuesta de modelo de gestión de riesgos de TI.	Modelado
Variable Dependiente: Procesos Comerciales	Serie de pasos o etapas que se siguen para cerrar una venta, desde que se atrae un nuevo prospecto a través del marketing, hasta el servicio que se le ofrece al cliente despues de su compra.	Validar el modelo de gestión de riesgos de TI mediante juicio de expertos.	Validación de la propuesta.	Porcentaje de validación de juicio de expertos.	Escala de Likert / Cuestionario
		Validar la utilidad del modelo propuesto para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción.	Validación de la propuesta.	Porcentaje de aceptación de utilidad del modelo aplicado en el caso de estudio.	Modelado

Tabla 1: Operacionalización de variables

2.4. Métodos, Técnicas e Instrumentos de Recolección de Datos

Variable	Técnicas	Instrumentos
Dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción.	Encuesta	Cuestionarios Entrevistas
	Observación	Documentos Estratégicos

Tabla 2: Métodos, Técnicas e instrumentos de recolección de datos

2.5. Técnicas de Procesamiento de Datos

Se elaboró un cuestionario, para conocer el estado actual sobre cómo se getionan los riesgos de tecnologías de información en las empresas distribuidoras de materiales de construcción de la región Lambayeque.

Se revisaron documentos estretegicos como el plan estratégico de la organización y plan estratégico de tecnologías de información.

El cuestionario teniendo en cuenta el marco de trabajo COBIT 5, el cual se aplicó a los jefes de tecnologías de Información de las empresas en estudio.

Para el procesamiento de los resultados obtenidos del cuestionario se utilizó el software Microsoft Excel 2016, con el cual obtuvimos gráficos, cuadros, tablas, etc.

2.6. Criterios de Selección

Los criterios seleccionados en el estudio para la presente tesis, se realizó obteniendo lo siguiente:

- El rubro de la empresa debe ser distribuidor de materiales de construcción.
- Su sede central debe estar ubicada en la ciudad de Chiclayo, la cual pertenece a la región Lambayeque.
- Contar con 10 años como mínimo en el mercado laboral dentro de la región Lambayeque.

2.7. Consideraciones Éticas

- La investigación utiliza palabras o resultados de diferentes investigaciones e investigadores, otorgando el reconocimiento que se merecen.
- La investigación proporciona datos reales.
- La investigación no manipula datos o procediminetos experimentales.
- La investigación debe tener la aprobación de todos los participantes del documento denominda consentimineto informado.
- La investigación protege la identidad de cada uno de los participantes en la encuestas y/o entrevistas.
- La investigación protege los datos de cada una de las empresas en estudio para mantener la condifencialidad de los mismos.
- La investigación no provoca actitudes que limiten en sus respuestas a todos los participantes.

CAPÍTULO III RESULTADOS Y DISCUSIÓN

3.1. Diagnóstico del Sector

Para el desarrollo de la presente investigación se realizó una descripción de las empresas del sector de ventas de materiales de construcción, un total de cuatro empresas fueron seleccionadas para realizar el diagnóstico del sector. Las empresas seleccionadas cuentan con más de 10 años de presencia en el mercado lambayecano, cuyas sedes principal en cada caso se ubica en la panamericana norte camino a la ciudad de Lambayeque. Para tres de estas empresas, el área de tecnologías de la información depende de la gerencia general, la cual les brinda las herramientas y el soporte necesario para el desarrollo de sus actividades de los procesos comerciales, sin embargo, se pudo identificar no cuentan formalizada un área dedicada a la gestión de riesgos de TI. Para más información detallada de las empresas que participan en el diagnóstico del sector (ver Anexo 1).

Se desarrolló un cuestionario de 15 preguntas tomando como referencia el marco de trabajo COBIT 5 para riesgos (ver Anexo 2), el cual se aplicó al jefe de TI de cada una de las cuatro empresas del sector en estudio, quienes dieron su consentimiento informado para la publicación de la presente investigación se cuidará la denominación de cada organización las cuales en adelante para la descripción e interpretación de los resultados obtenidos denominaremos Empresa 01, Empresa 02, Empresa 03, Empresa 04 (ver Anexo 3).

De acuerdo a los resultados obtenidos del cuestionario aplicado al jefe de TI de las empresas en estudio, se observa que el 75% manifiesta que no se ha establecido ningún marco de referencia para la gestión de riesgos, esto demuestra una escasa preocupación por formalizar una metodología a aplicar que permita identificar amenazas ante posibles riesgos y establecer adecuados niveles de protección sobre los recursos informáticos. El 50% de empresas en estudio ha logrado definir su alcance. Esto les permitirá conocer y proponer las herramientas y metodologías para una adecuada evaluación y gestión de riesgos. El 25% expone que ha logrado identificar y analizar los riesgos que la empresa puede aceptar para alcanzar sus objetivos estratégicos. El 100% indica que a nivel administrativo no existe área responsable comprometida en la gestión de riesgos de TI.

El 75% ha trabajado en identificar los riesgos, lo que les permite clasificarlos para poder ser revisados en cuanto a la probabilidad y consecuencia determinando su prioridad, para su tratamiento adecuado. El 100% ha identificado todos los activos tecnológicos que permita garantizar las operaciones comerciales y continuidad del negocio dentro de la organización. El 50% tiene claro que se debe establecer un enfoque detallado abarcando todos los eventos posibles de tal forma que puedan establecer una línea base para su gestión de riesgos. El 75% manifiesta que no se han identificados los controles que permitan minimizar la posibilidad de que un riesgo se materialice en una pérdida para la organización. El 75% expone que no se ha promovido la comprensión de los riesgos a los cuales se encuentra expuesta la organización, el mismo que les permitirá ejecutar distintas medidas que se puedan establecer para mitigar.

El 50% detalla que los empleados no son con conscientes sobre el uso de las tecnologías de información para poder identificar adecuadamente los riesgos. El 50% tiene identificado las actividades de control que permita garantizar las operaciones comerciales y continuidad del negocio dentro de la organización en caso de presentarse incidentes. El 75% señala que las partes interesadas no se encuentran informadas de manera que puedan tomar acciones y estrategias para el tratamiento

de los riesgos de TI. El 75% advierten que no se han establecido controles que permitan implementar planes de respuesta a los riesgos que se presenten. El 75% indica que no se tiene herramientas que permitan calcular los riesgos que se presentaron e impactaron o que no se lograron mitigar como parte de un indicador de efectividad en la gestión de riesgos. El 100% no ha establecido mecanismos para controlar los riesgos y mitigar el impacto dentro de la organización como parte de una adecuada gestión de riesgos.

Para mayor detalle acerca de los resultados obtenidos del cuestionario aplicado a los jefes de tecnologías de información de cada una de las empresas en estudio (ver Anexo 3).

Las gráficas obtenidas a partir de los resultados del cuestinario aplicado (ver Anexo 4).

3.2. Análisis de Estándares, Marcos de Trabajo y Metodologías Relacionadas

En este apartado se analizó los estándares, marcos de trabajo y metodologías existentes para la gestión de riesgos de tecnologías de la información, considerándose para este análisis las siguientes:

- ISO 31000:2018: Proporciona directrices para la gestión de riesgos.
- ISO 27005:2011: Proporciona directrices para la gestión de riesgos en la seguridad de la información.
- COBIT 5 para Riesgos: Marco de trabajo para la gestión de riesgos.
- MARGERIT v3.0: Metodología de análisis y gestión de riesgos de los sistemas de información.
- Octave: Conjunto de herramientas, técnicas y métodos para la evaluación del riesgo.

Para lo cual se realizó un analisis conceptual y un cuadro comparativo en relación a los estándares y metodologías antes mencionadas, el cual se utilizó para identificar fases coincidentes y aportaciones en gestión de riesgos que confieran en la realización de la propuesta del modelo según las necesidades y la realidad de las empresas distribuidoras de materiales de construcción (Ver Anexo 5).

3.3. Modelo Propuesto

Como resultado del análisis de estándares, metodologías y marcos de trabajo relacionados con la gestión de riesgos, se toma como base principal el estándar ISO31000:2018. Dicho estándar es adaptable a cualquier tipo de organización, en el que participa el compromiso de la alta dirección, proporcionando una gestión eficiente de los riesgos en todos los niveles dentro de la organización (ver Anexo 6).

La elaboración y el desarrollo del modelo propuesto consta de las siguientes fases:

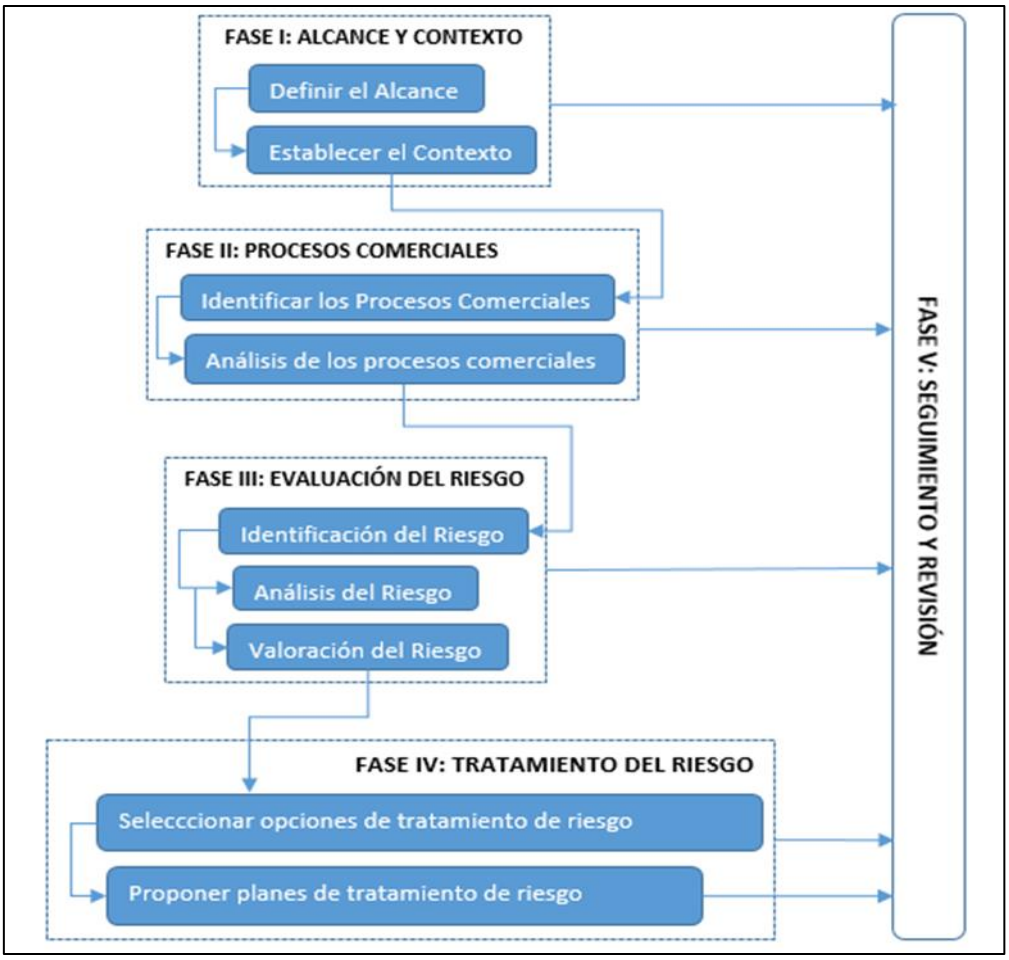


Figura 14: Modelo de Gestión de Riesgo propuesto tomando como referencia la ISO 31000:2018

3.4. Desarrollo del Modelo Propuesto

Fase I: Alcance y contexto

La organización debe definir el alcance de la gestión de riesgos, comprendiendo el contexto en que opera la organización en su entorno interno y externo.

Esta fase contempla las siguientes actividades:

1.1. Definición del alcance

En esta actividad esta actividad la organización deberá definir el alcance de la gestión de riesgo, el cual debe estar alineado con los objetivos de la organización, delimitando el proceso que será abarcado por la gestión del riesgo.

Entrada:

- Plan estratégico de la organización u otro documento de referencia de similares características.

Salida:

- La matriz de definición del alcance (Tabla N° 3).

Técnicas y Herramientas:

- Las técnicas a utilizar en la reunión podrán ser: lluvia de ideas, entrevista, entre otras.
- Las herramientas a utilizar en la reunión podrán ser: zoom, google meet, Skype, entre otras.

Procedimiento:

Se define el alcance con la participación de todos los interesados identificados, el cual será informado y aprobado por quien corresponda; se recomienda considerar:

- Indicar el área responsable del desarrollo del modelo de gestión de riesgos.
- Indicar la fecha de inicio del desarrollo del modelo de gestión de riesgos.

- Indicar la hora de inicio de la reunión.
- Indicar la hora término de la reunión.
- Indicar el tipo de reunión, si la reunión se realizó virtualmente debe indicar la plataforma utilizada, o de lo contrario si la reunión fue presencial debe indicar el lugar donde se desarrolló dicha reunión.
- Indicar los cargos de las áreas y firmas de los participantes en el desarrollo de la reunión.
- Describir los objetivos que se esperan alcanzar con el desarrollo del modelo de gestión de riesgos.
- Describir el alcance del modelo de gestión de riesgos, indicando a que proceso de la organización involucra.

LOGO	MATRIZ DE DEFINICIÓN DEL ALCANCE		Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.		
Nro.	**COMPONENTE**	**DESCRIPCIÓN**	
1	**AREA RESPONSABLE DEL COMPONENTE**	Indicar el área responsable.	
2	**FECHA**	Indicar la fecha de inicio.	
3	**HORA DE INICIO**	Indicar la hora de inicio de la reunión.	
4	**HORA DE FIN**	Indicar la hora término de la reunión.	
5	**TIPO DE TECNICA A UTILIZAR**	( ) Reunión Virtual, indicar plataforma: _____.	
		( ) Reunión Presencial, indicar el lugar: _____.	
6	**PARTICIPANTES**	Indicar participante 1.	Firma del participante 1.
		Indicar participante 2.	Firma del participante 2.
		Indicar participante 3.	Firma del participante 3.
		Indicar participante 4.	Firma del participante 4.
		Indicar participante 5.	Firma del participante 5.
		Indicar participante 6.	Firma del participante 6.
		Indicar participante 7.	Firma del participante 7.
		Indicar participante 8.	Firma del participante 8.
		Indicar participante n.	Firma del participante n.
7	**OBJETIVOS**	Describir los objetivos 1.	
		Describir los objetivos 2.	
		Describir los objetivos n.	
8	**ALCANCE**	Describir el alcance del modelo de gestión de riesgos, a que proceso de la organización involucra la gestión de riesgos.	

Tabla 3: Matriz de definición del alcance
Fuente: Elaboración Propia

LOGO	MATRIZ DE DEFINICIÓN DEL ALCANCE		Fecha: / /
	Objetivo: Definir el alcance de la gestión de riesgos.		
Nro.	**COMPONENTE**	**DESCRIPCIÓN**	
1	**AREA RESPONSABLE DEL COMPONENTE**	Área de Tecnologías de la información y Comunicaciones.	
2	**FECHA**	15 de diciembre del 2020.	
3	**HORA DE INICIO**	10:00 a.m.	
4	**HORA DE FIN**	11:45 a.m.	
5	**TIPO DE TECNICA A UTILIZAR**	(x) Reunión Virtual, indicar plataforma: ZOOM.	
		( ) Reunión Presencial, indicar el lugar: _____.	
6	**PARTICIPANTES**	Gerente General.	
		Gerente de Administración.	
		Gerente Comercial.	
		Jefes de Ventas.	
		Jefes Administrativos.	
		Jefes de Tecnologías de la Información y Comunicaciones.	
		Jefe de Contabilidad.	
		Jefe de Tesorería.	
		Jefe de Almacén.	
7	**OBJETIVOS**	Desarrollar una cultura de gestión de riesgos.	
		Realizar la identificación, análisis y valoración de los riesgos de los activos de TI, que dan soporte a los procesos comerciales de la organización.	
		Identificar amenazas y reducir vulnerabilidades presentadas en los activos de TI.	
8	**ALCANCE**	El procedimiento es aplicable para dar soporte a los procesos comerciales de la organización.	

Tabla 4: Ejemplo de matriz de definición del alcance

1.2. Contexto externo e interno

En esta actividad la organización debe establecer el entorno externo e interno sobre la cual se desarrolla, debiendo detallar el contexto específico sobre la actividad en la cual se va a aplicar el proceso de la gestión del riesgo.

- **Contexto interno**

  Entrada:

  - Plan estratégico de la organización u otro documento de referencia de similares características.
  - Manual de organización y funciones (MOF) de la organización u otro documento de referencia de similares características.
  - Organigrama de la organización u otro documento de referencia de similares características.
  - Inventario de activos de la organización u otro documento de referencia de similares características.

  Salida:

  - La matriz de contexto interno (Tabla N° 5).

  Técnicas y Herramientas:

  - Las técnicas a utilizar en la reunión podrán ser: lluvia de ideas, entrevista, entre otras.
  - Las herramientas a utilizar en la reunión podrán ser: zoom, google meet, Skype, entre otras.

  Procedimiento:

  Se define el contexto interno realizando una reunión con la participación de la gerencia comercial, jefes administrativos, jefes de ventas y el área de TI; se recomienda considerar:

  - Identificar la cultura organizacional, se define como un conjunto de normas y valores que las personas tienen en el interior de la

organización. Se considera la visión, misión, valores y partes interesadas de la organización.

- Identificar la estructura organizacional, se define como la división de actividades que se desarrollan en una empresa, las cuales son agrupadas en áreas. Se considera el organigrama de la organización.
- Identificar los objetivos organizacionales, se define como la situación deseada que la organización procura alcanzar, y que concretan el deseo contenido en su misión y visión a través de metas alcanzables. Se considera los objetivos estratégicos y organizacionales de la organización.
- Identificar los recursos, se define como el conjunto de activos tecnológicos que maneja la organización, los cuales permiten dar soporte a los procesos comerciales.

LOGO	MATRIZ DE CONTEXTO INTERNO	Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.	

- **Cultura organizacional**
  - **Misión**
  - **Visión**
  - **Valores**
  - **Partes Interesadas**
  - **Otras que se consideren necesarios.**

Fuente de información: Plan estratégico de la organización u otro documento de referencia de similares características.

- **Estructura Organizacional**

Fuente de información: Organigrama de la organización u otro documento de referencia de similares características.

- **Objetivos Organizacionales**
  - **Estratégico**
  - **Organizacional**
  - **Otras que se consideren necesarios.**

Fuente de información: Plan estratégico de la organización, Manual de organización y funciones (MOF) de la organización u otros documentos de referencia de similares características.

- **Recursos**

Fuente de información: Inventario de activos de la organización u otro documento de referencia de similares características.

Tabla 5: Matriz de contexto interno
Fuente: Elaboración Propia

LOGO	MATRIZ DE CONTEXTO INTERNO	Fecha: / /
	Objetivo: Establecer el contexto interno de la organización.	

❖ **Cultura organizacional**

- **Misión**

  Nos esforzamos por satisfacer las necesidades del cliente con productos al mejor precio junto con un servicio de alta calidad, con el compromiso de nuestros socios estratégicos; aplicando los valores de responsabilidad, confianza y honestidad.

- **Visión**

  Ser reconocida nacionalmente comercializando materiales de construcción, prometiendo atención personalizada a cada uno de nuestros clientes.

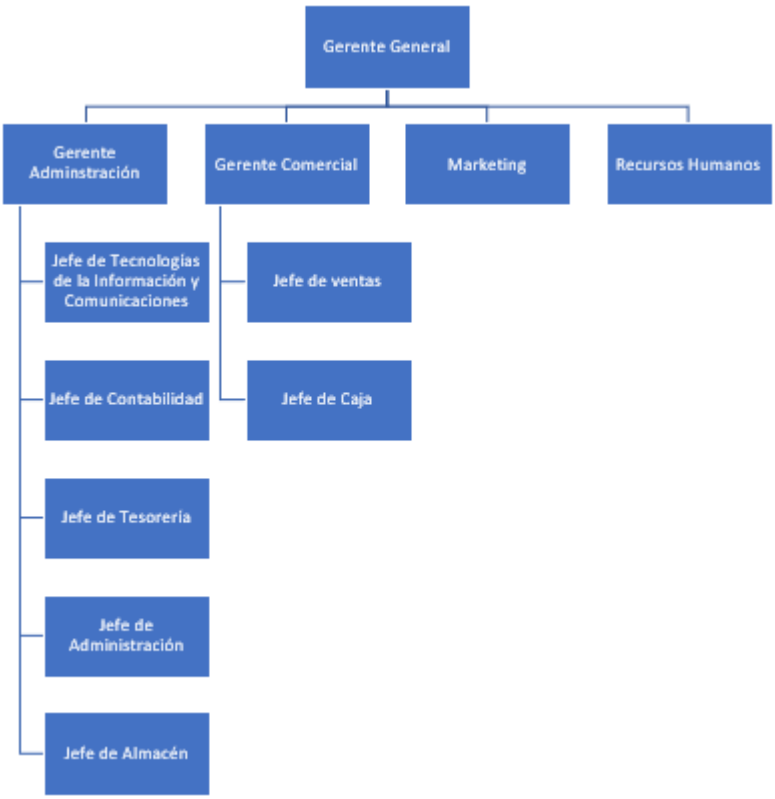
- **Valores**

  Responsabilidad, confianza y honestidad.

- **Partes Interesadas**

  Personal de gerencia, personal administrativo, personal comercial, socios estratégicos.

❖ **Estructura Organizacional**



LOGO	MATRIZ DE CONTEXTO INTERNO	Fecha: / /
	Objetivo: Establecer el contexto interno de la organización.	

❖ **Objetivos Organizacionales**

- **Estratégico**
  - Ampliar los actuales mercados.
  - Ampliar la cartera de clientes a nivel nacional.
  - Promover el desarrollo humano.
  - Gestionar estrategias para desarrollar proveedores comprometidos.
  - Mejorar y optimizar los procesos.
- **Organizacional**

  Consolidar el liderazgo de la organización en el mercado de venta de materiales de construcción, siendo reconocida a nivel nacional, brindando un servicio personalizado al cliente.

❖ **Recursos**

Se define como el conjunto de activos tecnológicos de información que dan soporte a los procesos comerciales de la organización como equipos informáticos, equipos de red, sistemas de información, servidores, etc.

Tabla 6: Ejemplo de matriz de contexto interno

- **Contexto externo**

  Entrada:

  - Superintendencia Nacional de Aduanas y de Administración Tributaria (Sunat).
  - Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi).
  - Instituto Nacional de Defensa Civil (Indeci).
  - Superintendencia de Banca y Seguros del Perú (SBS).
  - Banco Central de Reserva del Perú (BCRP).
  - Lista de oportunidades y amenazas.
  - Revista de activos tecnológicos (ESAN).
  - Otras instituciones relacionadas con el contexto externo.

  Salida:

  - La matriz de contexto externo (Tabla N° 7).

  Técnicas y Herramientas:

  - Las técnicas a utilizar en la reunión podrán ser: lluvia de ideas, entrevista, entre otras.
  - Las herramientas a utilizar en la reunión podrán ser: zoom, google meet, Skype, entre otras.

  Procedimiento:

  Se define el contexto externo realizando una reunión con la participación de la gerencia comercial, jefes administrativos, jefes de ventas y el área de TI; se recomienda considerar:

  - Identificar el ámbito legal, se define como los reglamentos y exigencias legales, donde al incumpliendo de ellas ponen en peligro la organización, como las normas tributarias y laborares.
  - Identificar el ámbito económico, se define como un conjunto de elementos relacionados con la economía, las variaciones en los precios en los productos de industria (tubos y perfiles

estructurales), incremento de la tasa de cambio, elevados impuestos a la renta.

- Identificar el ámbito competitivo, se define como el conjunto de items que resultan del análisis de la competencia directa, la cual afecta la economía y el desempeño de la organización.
- Identificar el ámbito tecnológico, se define como los factores relacionados con los cambios tecnológicos que se dan cada vez con mayor rapidez en estas organizaciones.

LOGO	MATRIZ DE CONTEXTO EXTERNO	Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.	

❖ **Ámbito Legal**

Fuente de información: Superintendencia Nacional de Aduanas y de Administración Tributaria (Sunat), Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi), Instituto Nacional de Defensa Civil (Indeci).

❖ **Ámbito Económico**

Fuente de información: Superintendencia de Banca y Seguros del Perú (SBS), Banco Central de Reserva del Perú (BCRP).

❖ **Ámbito Competitivo**

Fuente de información: Lista de oportunidades y amenazas.

❖ **Ámbito Tecnológico**

Fuente de información: Revista de activos tecnológicos (ESAN).

Tabla 7: Matriz de contexto externo
Fuente: Elaboración Propia

LOGO	MATRIZ DE CONTEXTO EXTERNO	Fecha: / /
	Objetivo: Establecer el contexto externo de la organización.	

❖ **Ámbito Legal**

- Legislación fiscal (SUNAT).
- Inspecciones técnicas de seguridad en edificaciones (INDECI).
- Protección al consumidor (INDECOPI).

❖ **Ámbito Económico**

- SBS.
- Economía del país.
- Banco central de reserva del Perú (BCRP).
- Entidades bancarias (BCP, Interbank, Continental, etc).

❖ **Ámbito Competitivo**

- Ferronor SAC.
- Steelmark SA.
- Quiroga SAC.
- 3A Expertos en Acero y Soldadura.

❖ **Ámbito Tecnológico**

Los avances tecnológicos que inciden en nuevos diseños y en la sofisticación de sistemas de información que promueven el uso de la tecnología que facilita la interacción entre grupos de interés, permite crear bases de datos a gran escala, lo cual le brinda a la organización la posibilidad de gestionar un mayor volumen de información y, finalmente, permite automatizar los procesos operacionales.

Tabla 8: Ejemplo de matriz de contexto externo

Fase II: Procesos comerciales

2.1. Identificar los procesos comerciales

Se debe identificar los procesos que apoyan la estrategia comercial de la organización, obteniendo la visión general de cada una de las actividades y los recursos que se necesitan.

Entrada:

- Plan estratégico de la organización u otro documento de referencia de similares características.

Salida:

- La matriz de identificación de procesos comerciales (Tabla N° 9).

Procedimiento:

- Identificar los procesos comerciales de la organización.

LOGO	**MATRIZ DE IDENTIFICACIÓN DE PROCESO COMERCIALES**			**Fecha: / /**
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.			
Nro.	**CÓDIGO**	**PROCESO**	**DESCRIPCIÓN**	**ÁREA**
1	Indicar el código con el siguiente formato: [P_"Nombre de proceso Abreviado"]	Indicar el nombre del proceso.	Indicar una breve descripción del proceso.	Indicar el área al cual pertenece el proceso

Tabla 9: Matriz de identificación de procesos comerciales
Fuente: Elaboración Propia

LOGO	MATRIZ DE IDENTIFICACIÓN DE PROCESO COMERCIALES			Fecha: / /
	Objetivo: Identificar los procesos comerciales de la organización.			
Nro.	**CÓDIGO**	**PROCESO**	**DESCRIPCIÓN**	**ÁREA**
1	[P_COM]	Proceso de compras	Consiste en contactar con los proveedores para adquirir un producto que permita disponibilidad stock en almacén.	Administración
2	[P_FAC]	Proceso de facturación	Consiste en concretar la venta a los clientes.	Ventas
3	[P_FPC]	Proceso de Actualización masiva de precios	Consiste en actualizar el precio de venta de los productos, y mantener la lista de precios actualizada.	Administración
4	[P_ALM]	Proceso de almacén	Consiste en recepcionar y almacenar los productos, adquiridos por el área de compras, así como entregar los productos vendidos a los clientes.	Almacén
5	[P_CIC]	Proceso de cierre de caja	Consiste en contabilizar diariamente, la entrada y salida de dinero de una determinada caja.	Ventas
6	[P_COB]	Proceso de cobranzas	Consiste en contactar a los clientes que mantienen deuda, para informar el estado de sus facturas y créditos, ofreciendo opciones de pago.	Ventas
7	[P_TES]	Proceso de tesorería	Consiste en realizar oportunamente los pagos a los proveedores.	Tesorería
8	[P_CON]	Proceso contable	Consiste en brindar información importante de las transacciones comerciales para la obtención de los estados financieros, permitiendo la toma oportuna de decisiones.	Contabilidad

Tabla 10: Ejemplo de matriz de identificación de procesos comerciales

2.2. Análisis de los procesos comerciales

Son un conjunto de pasos o actividades que los empleados deben seguir para ofrecer valor al cliente, garantizando la gestión eficiente del tiempo en las áreas de la organización.

Entrada:

- La matriz de identificación de procesos comerciales (Tabla N° 9).

Salida:

- La matriz para identificar las actividades de los procesos comerciales (Tabla N° 11).

Procedimiento:

- Identificar el proceso comercial.
- Identificar el responsable de cada proceso comercial.
- Describir cada una de las actividades de cada proceso comercial.
- Marcar con un aspa (X), los activos de TI que interactúan en cada proceso comercial, para lo cual se utilizará las siguientes abreviaturas de los siguientes activos de TI:
  - ✓ COE: Computadora de escritorio.
  - ✓ LAP: Laptop.
  - ✓ TAB: Tablet.
  - ✓ IMP: Impresora.
  - ✓ DIA: Dispositivo de almacenamiento (USB).
  - ✓ SAI: Servicio de acceso a internet.
  - ✓ SCE: Servicio de correo electrónico.
  - ✓ SIE: Sistema ERP.
  - ✓ SIV: Sistema web de ventas.

  Esta lista de activos puede variar según la necesidad de la organización.

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
Indicar el nombre del proceso 1	Indicar el responsable del proceso 1	Describir actividad 1.									
		Describir actividad 2.									
		Describir actividad n.									
Indicar el nombre del proceso 2	Indicar el responsable del proceso 2	Describir actividad 1.									
		Describir actividad 2.									
		Describir actividad n.									
Indicar el nombre del proceso 3	Indicar el responsable del proceso 3	Describir actividad n.									
Indicar el nombre del proceso 4	Indicar el responsable del proceso 4	Describir actividad 1.									
		Describir actividad 2.									
		Describir actividad n.									
Indicar el nombre del proceso 5	Indicar el responsable del proceso 5	Describir actividad n.									
Indicar el nombre del proceso 6	Indicar el responsable del proceso 5	Describir actividad 1.									
		Describir actividad 2.									
		Describir actividad n.									
Indicar el nombre del proceso 7	Indicar el responsable del proceso 7	Describir actividad 1.									
		Describir actividad 2.									
		Describir actividad n.									
Indicar el nombre del proceso n	Indicar el responsable del proceso n	Describir actividad 1.									
		Describir actividad 2.									
		Describir actividad n.									

Tabla 11: Matriz para identificar las actividades de los procesos comerciales
Fuente: Elaboración Propia

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Identificar las actividades de los procesos comerciales.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
Proceso de Compras	Jefe Administración	Registrar proveedores en el módulo de compras del sistema ERP.	X							X	
		Cotizar precios compra de productos a diferentes proveedores.	X			X		X	X		
		Registra documentos de compra (facturas, notas de crédito, notas de débito) en el módulo de compras del sistema ERP.	X			X				X	
		Aprobación de descuentos de venta en el módulo de facturación del sistema ERP.	X							X	
		Aprobación de cotizaciones generadas por los ejecutivos comerciales en el sistema web de ventas.	X			X					X
		Asignación de ventas de ejecutivos comerciales en el módulo de facturación del sistema ERP.	X							X	
		Cotizar precios de ventas a los clientes en el módulo de facturación del sistema ERP, ya se presencialmente o por correo electrónico.	X			X		X	X	X	
		Consultar reportes (registro de compras, ventas por vendedor, lista de precios) en el sistema ERP.	X			X				X	
Proceso de Facturación	Jefe de ventas	Gestor comercial registra clientes en módulo de facturación del sistema ERP.	X							X	
		Gestor comercial cotiza precios de venta a los clientes en el módulo de facturación del sistema ERP, ya se presencialmente o por correo electrónico.	X			X		X	X	X	
		Gestor comercial registra documentos de venta (facturas, boletas, notas de crédito, notas de débito) en el módulo de facturación del sistema ERP.	X			X				X	
		Gestor comercial contabiliza documentos de ventas (facturas, boletas, notas de crédito, notas de débito) en el módulo de facturación del sistema ERP.	X							X	
		Gestor comercial genera guías de remisión en el módulo de almacén del sistema ERP.	X			X				X	
		Gestor comercial genera guías de transportista en el módulo de almacén del sistema ERP.	X			X				X	

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Identificar las actividades de los procesos comerciales.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
		Ejecutivo comercial externo registra clientes en el sistema web de ventas.		X	X			X			X
		Ejecutivo comercial externo registra hoja de ruta (diariamente) en el sistema web de ventas.		X	X		X	X			X
		Ejecutivo comercial externo cotiza precios de venta en el sistema web de ventas, ya se presencialmente o por correo electrónico.		X	X	X		X	X		X
		Ejecutivo comercial externo registra una venta en el sistema web de ventas.		X	X			X			X
		Consultar reportes (diario de caja, ventas de caja, cuentas por cobrar, lista de precios, ventas por vendedor) en el sistema ERP.		X	X	X				X	X
Proceso de Actualización masiva de precios	Jefe Administración	Actualiza precios de venta en el módulo de actualización masiva de precios del sistema ERP.	X			X				X	
Proceso de almacén	Jefe de Almacen	Generar guías internas en el módulo de almacén del sistema ERP.	X			X				X	
		Crear productos en el módulo de almacén del sistema ERP.	X							X	
		Registrar traslados de productos a otros almacenes de la organización, utilizando el módulo de almacén del sistema ERP.	X			X		X	X	X	
		Consultar reportes (compras de mercadería, stock de productos).	X			X				X	
Proceso de cierre de caja	Jefe de ventas	Registrar el cierre en el módulo de cierre de caja del sistema ERP.	X							X	
Proceso de cobranzas	Jefe de ventas	Registrar línea de crédito en el módulo de cobranzas del sistema ERP.	X							X	
		Cancelar documentos de venta en el módulo de cobranzas del sistema ERP.	X					X	X	X	
		Cancelación de gastos de movilidad en el módulo de cobranzas del sistema ERP.	X					X	X	X	
		Consultar reportes (cuentas por cobrar) en el sistema ERP.	X			X				X	
Proceso de tesorería	Jefe de Tesorería	Registrar proveedores en el módulo de compras del sistema ERP.	X							X	
		Registro de gastos en el módulo de tesorería del sistema ERP.	X							X	

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Identificar las actividades de los procesos comerciales.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
		Cancelar documentos de compra en el módulo de tesorería del sistema ERP.	X					X	X	X	
		Cancelar documentos de gastos en el módulo de tesorería del sistema ERP.	X							X	
		Consultar reportes (cuentas por pagar).	X			X				X	
Proceso contable	Jefe de Contabilidad	Registrar asientos en el módulo contable del sistema ERP.	X							X	
		Aprobación de aperturas de caja en el módulo de cierre de caja del sistema ERP.	X					X	X	X	
		Anulación de documentos de venta (facturas, boletas, notas de crédito, notas de débito) en el módulo de facturación del sistema ERP.	X					X	X	X	
		Anulación de documentos de compra (facturas, notas de crédito, notas de débito) en el módulo de compras del sistema ERP.	X					X	X	X	
		Consulta de reportes (cuentas por cobrar, cuentas por pagar, ventas de caja, registro de compra, estados financieros).	X			X				X	

Tabla 12: Ejemplo de matriz para identificar las actividades de los procesos comerciales

Fase III: Evaluación del riesgo

En esta fase se analizan los riesgos que afrontan los activos de TI que dan soporte a los procesos comerciales y que afectarían en el logro de los objetivos de la organización.

Esta fase contempla las siguientes actividades:

3.1. Identificar del riesgo

En esta actividad su objetivo es identificar y valorar los activos de TI, que dan soporte a los procesos comerciales de la organización, para determinar las amenazas y vulnerabilidades a los que están expuestos.

3.1.1. Identificación de activos

La clasificación de los activos de TI, se formula tomando en cuenta las recomendaciones de la metodología Magerit v3.0.

Entrada:

- Lista de activos de TI que intervienen en los procesos comerciales de la organización, la cual es obtenida de la fase 2.

Salida:

- La matriz de identificación de activos de TI (Tabla N° 13).

Procedimiento:

- Describir el objetivo de la identificación de activos de TI.
- Clasificar cada activo de TI, siguiendo las siguientes consideraciones:
  - **[P] Proceso de Negocio**

    Este tipo de activo son todos los procesos que para las empresas distribuidoras de materiales de

construcción están relacionados con los procesos comerciales.

- ❖ **[S] Servicios**

  Este activo tiene por objetivo satisfacer las necesidades de los usuarios dentro de la organización. Los servicios pueden ser proporcionados por terceros.

- ❖ **[SW] Software**

  Este activo se refiere a programas, aplicativos, software desarrollado dentro de la organización, los cuales permiten a los usuarios realizar diferentes actividades relacionadas a los procesos comerciales de la organización.

- ❖ **[HW] Hardware**

  Este activo se refiere a los bienes materiales que soportan tecnológicamente los servicios prestados a los usuarios.

- ❖ **[SIN] Soporte de información**

  Este activo se refiere a los medios físicos o lógicos que permiten resguardar la información de la organización.

- Establecer un código para cada activo de TI con el siguiente formato: [Clasificación del activo_"Nombre del activo abreviado"].
- Identificar el área al cual pertenece el activo de TI.
- Identificar el propietario del activo de TI.

LOGO	MATRIZ DE IDENTIFICACIÓN DE ACTIVOS DE TI				Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.				
Nro.	**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	**ÁREA**	**PROPIETARIO**
1	Indicar la clasificación del activo de TI.	Indicar el código del activo de TI.	Indicar el nombre del activo de TI.	Indicar el área al que pertenece el activo	Indicar el propietario del activo.

Tabla 13: Matriz de identificación de activos de TI
Fuente: Elaboración Propia

LOGO	MATRIZ DE IDENTIFICACIÓN DE ACTIVOS DE TI				Fecha: / /
	Objetivo: Listar los activos que intervienen en los procesos comerciales.				
Nro.	**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	**ÁREA**	**PROPIETARIO**
1	Proceso	[P_COM]	Proceso de compras	Administración	Jefe Administración
2	Proceso	[P_FAC]	Proceso de facturación	Ventas	Jefe Ventas
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Administración	Jefe Administración
4	Proceso	[P_ALM]	Proceso de almacén	Almacén	Jefe de Almacén
5	Proceso	[P_CIC]	Proceso de cierre de caja	Ventas	Jefe Ventas
6	Proceso	[P_COB]	Proceso de cobranzas	Ventas	Jefe de Ventas
7	Proceso	[P_TES]	Proceso de tesorería	Tesorería	Jefe de Tesorería
8	Proceso	[P_CON]	Proceso contable	Contabilidad	Jefe de Contabilidad
9	Hardware	[HW_COE]	Computadoras de escritorio	TIC's	Jefe de Tic's
10	Hardware	[HW_LAP]	Lapto's	TIC's	Jefe de Tic's
11	Hardware	[HW_TAB]	Tablet's	TIC's	Jefe de Tic's
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	TIC's	Jefe de Tic's
13	Hardware	[HW_SWI]	Switch	TIC's	Jefe de Tic's
14	Hardware	[HW_ACP]	Access Point	TIC's	Jefe de Tic's
15	Hardware	[HW_CAE]	Cableado esrtucturado de red	TIC's	Jefe de Tic's
16	Hardware	[HW_FIR]	Equipo firewall	TIC's	Jefe de Tic's
17	Hardware	[HW_UPS]	UPS	TIC's	Jefe de Tic's
18	Hardware	[HW_IMP]	Impresoras	TIC's	Jefe de Tic's
19	Hardware	[HW_SEA]	Servidor de aplicaciones	TIC's	Jefe de Tic's
20	Hardware	[HW_SED]	Servidor de base datos ERP	TIC's	Jefe de Tic's
21	Software	[SW_BDE]	Base de datos del sistema ERP	TIC's	Jefe de Tic's

LOGO	MATRIZ DE IDENTIFICACIÓN DE ACTIVOS DE TI				Fecha: / /
	Objetivo: Listar los activos que intervienen en los procesos comerciales.				
Nro.	**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	**ÁREA**	**PROPIETARIO**
22	Software	[SW_SIE]	Sistema ERP	TIC's	Jefe de Tic's
23	Software	[SW_SIV]	Sistema web de ventas	TIC's	Jefe de Tic's
24	Software	[SW_LIS]	Licencias de software	TIC's	Jefe de Tic's
25	Software	[SW_PAW]	Página web de la organización	TIC's	Jefe de Tic's
26	Soporte de información	[SIN_BBD]	Backup de base de datos	TIC's	Jefe de Tic's
27	Servicio	[S_SCE]	Servicio de correo electrónico	TIC's	Jefe de Tic's
28	Servicio	[S_SAI]	Servicio de acceso a internet	TIC's	Jefe a Tic's
29	Servicio	[S_WIF]	Servicio de wifi	TIC's	Jefe de Tic's
30	Servicio	[S_PAW]	Servicio de página web	TIC's	Jefe de Tic's

Tabla 14: Ejemplo de matriz de identificación de activos de TI

3.1.2. Valoración de los activos

Una vez culminada la actividad de inventario de activos, se debe valorar los activos de TI de acuerdo al grado de importancia que tienen para la organización. Para el proceso de valoración, se sugiere usar la Escala de Likert, que permite medir los criterios de valoración.

Entrada:

- La matriz de identificación de activos de TI (Tabla N° 13).

Salida:

- La matriz de valoración de activos de TI (Tabla N° 17).

Procedimiento:

- Determinar los criterios de valoración de los activos de TI considerando los siguientes criterios:

- **Confidencialidad (C)**

  Información sensible y/o privada que no es accesible a cualquier persona que no sea autorizada para verla (Tabla N° 15).

- **Integridad (I)**

  Propiedad de salvaguardar la autenticidad y/o exactitud de un activo de información para que no sea alterado de forma no autorizada (Tabla N° 15).

- **Disponibilidad (D)**

  Es la frecuencia con la que debe estar disponible un activo y listo para su uso (Tabla N° 15).

- Determinar el nivel de valoración de los activos de TI, el cual se obtiene de la sumatoria de los valores establecidos para cada criterio de valoración, tal y como se muestra en la siguiente relación:

Nivel de Valoración = Confidencialidad + Integridad + Disponibilidad

El resultado obtenido en la ecuación, debe establecer el nivel de valoración (Tabla N° 16).

VALORACIÓN DE CRITERIOS DE LOS ACTIVOS DE TI			
VALOR	**CONFIDENCIALIDAD (C)**	**INTEGRIDAD (I)**	**DISPONIBILIDAD (D)**
5 Muy Alto	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas.	Tiene que estar correcto y completo al menos en un 99%.	Debe estar disponible al menos el 99% del tiempo.
4 Alto	Los daños serían relevantes, el incidente implicaría a otros procesos.	Tiene que estar correcto y completo al menos en un 75%.	Debe estar disponible al menos el 75% del tiempo.
3 Medio	Daños bajos, el incidente no transcendiera del proceso afectado.	Tiene que estar correcto y completo al menos en un 50%.	Debe estar disponible al menos el 50% del tiempo.
2 Bajo	Daños muy bajos, el incidente no trascendiera del proceso afectado.	No es relevante los errores que tenga o la información que falte.	Debe estar disponible al menos el 10% del tiempo.
1 Muy Bajo	No aplica./ No es relevante para la organización.	No aplica./ No es relevante para la organización.	No aplica./ No es relevante para la organización.

Tabla 15: Valoración de criterios de los activos de TI
Fuente: Elaboración Propia

NIVEL DE VALORACIÓN DE LOS ACTIVOS DE TI	
RANGO (resultado de la sumatoria)	**NIVEL DE CRITICIDAD**
De 1 a 3	Muy Bajo
De 4 a 6	Bajo
De 7 a 9	Medio
De 10 a 12	Alto
De 13 a 15	Muy Alto

Tabla 16: Nivel valoración de los activos de TI
Fuente: Elaboración Propia

LOGO	**MATRIZ DE VALORACIÓN DE ACTIVOS DE TI**							**Fecha: / /**
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.							
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**ESCALA DE VALORACIÓN DE CRITERIOS**			**NIVEL DE VALORACIÓN**	
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**	**C**	**I**	**D**	**TOTAL**	**NIVEL**
1	Indicar la clasificación del activo de TI.	Indicar el código del activo de TI.	Indicar el nombre del activo de TI.	Indicar el valor de confidencialidad, de acuerdo a la tabla 25.	Indicar el valor de integridad de, acuerdo a la tabla 25.	Indicar el valor de disponibilidad, de acuerdo a la tabla 25.	Indicar la sumatoria de los criterios.	Indicar el valor del nivel de valoración del activo, de acuerdo a la tabla 25.

Tabla 17: Matriz de valoración de activos de TI
Fuente: Elaboración Propia

LOGO	MATRIZ DE VALORACIÓN DE ACTIVOS DE TI							Fecha: / /
	Objetivo: Valorizar los activos de TI, considerando los criterios de confidencialidad, integridad y disponibilidad.							
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**ESCALA DE VALORACIÓN DE CRITERIOS**			**NIVEL DE VALORACIÓN**	
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**	**C**	**I**	**D**	**TOTAL**	**NIVEL**
1	Proceso	[P_COM]	Proceso de compras	4	5	5	14	Muy Alto
2	Proceso	[P_FAC]	Proceso de facturación	4	5	5	14	Muy Alto
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	5	5	5	15	Muy Alto
4	Proceso	[P_ALM]	Proceso de almacén	...	...	...	...	...
5	Proceso	[P_CIC]	Proceso de cierre de caja	...	...	...	...	...
6	Proceso	[P_COB]	Proceso de cobranzas	...	...	...	...	...
7	Proceso	[P_TES]	Proceso de tesorería					
8	Proceso	[P_CON]	Proceso contable					
9	Hardware	[HW_COE]	Computadoras de escritorio					
10	Hardware	[HW_LAP]	Laptop's					
11	Hardware	[HW_TAB]	Tablet's					
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB					
13	Hardware	[HW_SWI]	Switch					
14	Hardware	[HW_ACP]	Access Point					
15	Hardware	[HW_CAE]	Cableado esrtucturado de red					
16	Hardware	[HW_FIR]	Equipo firewall					
17	Hardware	[HW_UPS]	UPS					
18	Hardware	[HW_IMP]	Impresoras					
19	Hardware	[HW_SEA]	Servidor de aplicaciones					
20	Hardware	[HW_SED]	Servidor de base datos ERP					
21	Software	[SW_BDE]	Base de datos del sistema ERP					
22	Software	[SW_SIE]	Sistema ERP					
23	Software	[SW_SIV]	Sistema web de ventas					
24	Software	[SW_LIS]	Licencias de software					
25	Software	[SW_PAW]	Página web de la organización					

LOGO	MATRIZ DE VALORACIÓN DE ACTIVOS DE TI							Fecha: / /
	Objetivo: Valorizar los activos de TI, considerando los criterios de confidencialidad, integridad y disponibilidad.							
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**ESCALA DE VALORACIÓN DE CRITERIOS**			**NIVEL DE VALORACIÓN**	
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**	**C**	**I**	**D**	**TOTAL**	**NIVEL**
26	Soporte de información	[SIN_BBD]	Backup de base de datos					
27	Servicio	[S_SCE]	Servicio de correo electrónico					
28	Servicio	[S_SAI]	Servicio de acceso a internet					
29	Servicio	[S_WIF]	Servicio de wifi					
30	Servicio	[S_PAW]	Servicio de página web					

Tabla 18: Ejemplo de matriz de valoración de activos de TI

3.1.3. Identificar las amenazas

Es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto periodo de tiempo en un sitio dado.

Entrada:

- La matriz de identificación de activos de TI (Tabla N° 13).

Salida:

- La matriz de identificar amenazas (Tabla N° 19).

Procedimiento:

- Determinar las amenazas a las que están expuestos cada activo de TI.

LOGO	MATRIZ DE IDENTIFICAR AMENAZAS			Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.			
Nro.	IDENTIFICACIÓN DE ACTIVO			AMENAZAS
	CLASIFICACIÓN	CODIGO	ACTIVO	
1	Indicar la clasificación del activo de TI.	Indicar el código del activo de TI	Indicar el nombre del activo de TI.	Describir las amenazas que podría afectar el activo.

Tabla 19: Matriz de identificar amenazas
Fuente: Elaboración Propia

LOGO	MATRIZ DE IDENTIFICAR AMENAZAS			Fecha: / /
	Objetivo: Determinar las amenazas a las que están expuestos los activos de TI.			
Nro.	IDENTIFICACIÓN DE ACTIVO			AMENAZAS
	CLASIFICACIÓN	CODIGO	ACTIVO	
1	Proceso	[P_COM]	Proceso de compras	Registro de datos errados en el ingreso de una factura de compra
2	Proceso	[P_FAC]	Proceso de facturación	Pérdida de dinero, debido a fallas en el sistema
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Registro de datos errados en la actualización masiva de precios
4	Proceso	[P_ALM]	Proceso de almacén	…
5	Proceso	[P_CIC]	Proceso de cierre de caja	…
6	Proceso	[P_COB]	Proceso de cobranzas	…
7	Proceso	[P_TES]	Proceso de tesorería	
8	Proceso	[P_CON]	Proceso contable	
9	Hardware	[HW_COE]	Computadoras de escritorio	
10	Hardware	[HW_LAP]	Laptop's	
11	Hardware	[HW_TAB]	Tablet's	
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	
13	Hardware	[HW_SWI]	Switch	
14	Hardware	[HW_ACP]	Access Point	
15	Hardware	[HW_CAE]	Cableado esrtucturado de red	
16	Hardware	[HW_FIR]	Equipo firewall	
17	Hardware	[HW_UPS]	UPS	
18	Hardware	[HW_IMP]	Impresoras	
19	Hardware	[HW_SEA]	Servidor de aplicaciones	
20	Hardware	[HW_SED]	Servidor de base datos ERP	
21	Software	[SW_BDE]	Base de datos del sistema ERP	
22	Software	[SW_SIE]	Sistema ERP	

LOGO	MATRIZ DE IDENTIFICAR AMENAZAS			Fecha: / /
	Objetivo: Determinar las amenazas a las que están expuestos los activos de TI.			
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**	
23	Software	[SW_SIV]	Sistema web de ventas	
24	Software	[SW_LIS]	Licencias de software	
25	Software	[SW_PAW]	Página web de la organización	
26	Soporte de información	[SIN_BBD]	Backup de base de datos	
27	Servicio	[S_SCE]	Servicio de correo electrónico	
28	Servicio	[S_SAI]	Servicio de acceso a internet	
29	Servicio	[S_WIF]	Servicio de wifi	
30	Servicio	[S_PAW]	Servicio de página web	

Tabla 20: Ejemplo de matriz de identificar amenazas

3.1.4. Identificar las vulnerabilidades

Es el grado de pérdida de un elemento o grupo de elementos bajo riesgo, resultado de la probable ocurrencia de un suceso desastroso.

Entrada:

- La matriz de identificar amenazas (Tabla N° 19).

Salida:

- La matriz de identificar vulnerabilidades (Tabla N° 21).

Procedimiento:

- Determinar las vulnerabilidades de las amenazas a las que están expuestos cada activo de TI.

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
1	Indicar la clasificación del activo de TI.	Indicar el código del activo de TI	Indicar el nombre del activo de TI.	Describir las amenazas que podría afectar el activo.	Describir la vulnerabilidad que expone al activo a la amenaza.

Tabla 21: Matriz de identificar vulnerabilidades
Fuente: Elaboración Propia

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
1	Proceso	[P_COM]	Proceso de compras	Registro de datos errados en el ingreso de una factura de compra	Falta de validación de datos de entrada
2	Proceso	[P_FAC]	Proceso de facturación	Pérdida de dinero, debido a fallas en el sistema	Carencia de procedimientos para revisar lo facturado
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Registro de datos errados en la actualización masiva de precios	Falta de validación de datos de entrada
4	Proceso	[P_ALM]	Proceso de almacén	…	…
5	Proceso	[P_CIC]	Proceso de cierre de caja	…	…
6	Proceso	[P_COB]	Proceso de cobranzas	…	…
7	Proceso	[P_TES]	Proceso de tesorería		
8	Proceso	[P_CON]	Proceso contable		
9	Hardware	[HW_COE]	Computadoras de escritorio		
10	Hardware	[HW_LAP]	Laptop's		
11	Hardware	[HW_TAB]	Tablet's		
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB		
13	Hardware	[HW_SWI]	Switch		
14	Hardware	[HW_ACP]	Access Point		
15	Hardware	[HW_CAE]	Cableado esrtucturado de red		

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	IDENTIFICACIÓN DE ACTIVO			AMENAZAS	VULNERABILIDADES
	CLASIFICACIÓN	CODIGO	ACTIVO		
16	Hardware	[HW_FIR]	Equipo firewall		
17	Hardware	[HW_UPS]	UPS		
18	Hardware	[HW_IMP]	Impresoras		
19	Hardware	[HW_SEA]	Servidor de aplicaciones		
20	Hardware	[HW_SED]	Servidor de base datos ERP		
21	Software	[SW_BDE]	Base de datos del sistema ERP		
22	Software	[SW_SIE]	Sistema ERP		
23	Software	[SW_SIV]	Sistema web de ventas		
24	Software	[SW_LIS]	Licencias de software		
25	Software	[SW_PAW]	Página web de la organización		
26	Soporte de información	[SIN_BBD]	Backup de base de datos		
27	Servicio	[S_SCE]	Servicio de correo electrónico		
28	Servicio	[S_SAI]	Servicio de acceso a internet		
29	Servicio	[S_WIF]	Servicio de wifi		
30	Servicio	[S_PAW]	Servicio de página web		

Tabla 22:Ejemplo de matriz de identificar vulnerabilidades

3.2. Análisis del riesgo

El análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo.

En esta actividad se recomienda utilizar técnicas como: cuestionarios, lluvia de ideas, entre otros, en el que se puede identificar los riesgos asociados a cada activos de TI, así sus amenazas y vulnerabilidades, que afecten el desarrollo de las actividades de los procesos comerciales.

Entrada:

- La matriz de identificar vulnerabilidades (Tabla N° 21).

Salida:

- La matriz de análisis de los riesgos (Tabla N° 26).

Procedimiento:

- Determinar la probabilidad de ocurrencia de las vulnerabilidades de los activos de TI, para lo cual se debe asignar un valor (Tabla N° 23).
- Determinar el nivel de impacto de las vulnerabilidades de los activos de TI, para lo cual se debe asignar un valor (Tabla N° 24).
- Determinar el nivel del riesgo, mediante la multiplicación entre la probabilidad de ocurrencia y nivel de impacto, como se expresa en la siguiente ecuación:

  Riesgo = Probabilidad de ocurrencia X nivel de impacto

- En base a la determinación de la valoración de probabilidad de ocurrencia y nivel de impacto se plantea una estructura semaforizada que permite destacar mediante colores los niveles de riesgos para ser identificados de forma rápida y oportuna (Tabla N° 25).

VALORACIÓN DE PROBABILIDAD DE OCURRENCIA		
VALOR	**PROBABILIDAD**	**FRECUENCIA**
5	Casi Cierto	Ocurre diariamente durante un mes.
4	Muy Posible	Ocurre una sola vez durante el mes.
3	Posible	Ocurre una vez al año.
2	Raro	Ocurre una vez cada 5 años.
1	Casi Imposible	No ocurre en un período de 5 años.

Tabla 23: Valoración de probabilidad de ocurrencia
Fuente: Elaboración Propia

VALORACIÓN DE NIVEL DE IMPACTO		
VALOR	**IMPACTO**	**DESCRIPCIÓN**
5	Catastrófico	Se suspenden todas las actividades de los procesos comerciales de la organización.
4	Mayor	Se suspende la atención a los clientes, debido a una caída significativa de las operaciones, el cual afecta los procesos comerciales de la organización.
3	Moderado	Retrasan la ejecución de los procesos comerciales de la organización.
2	Menor	Limita parcialmente la ejecución de los procesos comerciales de la organización.
1	Insignificante	No afecta la ejecución de los procesos comerciales.

Tabla 24: Valoración del nivel de impacto
Fuente: Elaboración Propia

VALORACIÓN DE NIVEL DEL RIESGO		
NIVEL	**RANGO**	**DESCRICPIÓN**
3	De 12 a 25	Alto
2	De 5 a 10	Moderado
1	De 1 a 4	Bajo

Tabla 25: Valoración de nivel del riesgo
Fuente: Elaboración Propia

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS										Fecha: / /
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
1	Indicar la clasificación del activo de TI.	Indicar el código del activo de TI	Indicar el nombre del activo de TI.	Describir la amenaza que podría afectar el activo.	Describir la vulnerabilidad que expone al activo a la amenaza.	Indicar el valor de acuerdo a la tabla 33 de valoración de probabilidad.	Indicar el valor de acuerdo a la tabla 34 valoración de impacto.	Probalidad x Impacto	Código del riesgo.	Indicar el valor de acuerdo a la tabla 35 de nivel de riesgo.	Indicar la descripción del valor del nivel de riesgo.

Tabla 26: Matriz de análisis de los riesgos
Fuente: Elaboración Propia

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS										Fecha: / /
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
1	Proceso	[P_COM]	Proceso de compras	Registro de datos errados en el ingreso de una factura de compra	Falta de validación de datos de entrada	4	4	16	R1	3	Alto
2	Proceso	[P_FAC]	Proceso de facturación	Pérdida de dinero, debido a fallas en el sistema	Carencia de procedimientos para revisar lo facturado	3	3	9	R2	2	Moderado
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Registro de datos errados en la actualización masiva de precios	Falta de validación de datos de entrada	4	5	20	R3	3	Alto
4	Proceso	[P_ALM]	Proceso de almacén	…	…	…	…	…	…	…	…
5	Proceso	[P_CIC]	Proceso de cierre de caja	…	…	…	…	…	…	…	…
6	Proceso	[P_COB]	Proceso de cobranzas	…	…	…	…	…	…	…	…
7	Proceso	[P_TES]	Proceso de tesorería								
8	Proceso	[P_CON]	Proceso contable								
9	Hardware	[HW_COE]	Computadoras de escritorio								

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS									Fecha: / /	
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
10	Hardware	[HW_LAP]	Laptop's								
11	Hardware	[HW_TAB]	Tablet's								
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB								
13	Hardware	[HW_SWI]	Switch								
14	Hardware	[HW_ACP]	Access Point								
15	Hardware	[HW_CAE]	Cableado esrtucturado de red								
16	Hardware	[HW_FIR]	Equipo firewall								
17	Hardware	[HW_UPS]	UPS								
18	Hardware	[HW_IMP]	Impresoras								
19	Hardware	[HW_SEA]	Servidor de aplicaciones								

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS									Fecha: / /
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.									
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**	
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**
20	Hardware	[HW_SED]	Servidor de base datos ERP							
21	Software	[SW_BDE]	Base de datos del sistema ERP							
22	Software	[SW_SIE]	Sistema ERP							
23	Software	[SW_SIV]	Sistema web de ventas							
24	Software	[SW_LIS]	Licencias de software							
25	Software	[SW_PAW]	Página web de la organización							
26	Soporte de información	[SIN_BBD]	Backup de base de datos							
27	Servicio	[S_SCE]	Servicio de correo electrónico							
28	Servicio	[S_SAI]	Servicio de acceso a internet							

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS									Fecha: / /	
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
29	Servicio	[S_WIF]	Servicio de wifi								
30	Servicio	[S_PAW]	Servicio de página web								

Tabla 27: Ejemplo de matriz de análisis de los riesgos

3.3. Valoración del riesgo

En esta actividad, para la valoración del riesgo se procede a comparar los resultados del análisis del riesgo con sus criterios para determinar si el riesgo o su magnitud son aceptables, tolerables e intolerables.

Entrada:

- La matriz de análisis de los riesgos (Tabla N° 26).

Salida:

- La matriz de valoración del riesgo (Tabla N° 29).

Procedimiento:

- Determinar la priorización del riesgo identificado según el nivel de impacto y probabilidad de ocurrencia, para ello se definirá la ubicación del riesgo dentro de un mapa de calor que permita facilitar la identificación de la prioridad del riesgo para una correcta toma de decisiones (Figura N° 15).

  Para ubicar un riesgo dentro del mapa de calor, se debe considerar los puntajes establecidos para la probabilidad de ocurrencia y el nivel de impacto en la actividad de análisis del riesgo. Según esto, el riesgo se ubica en la zona verde, amarillo o roja indicando el nivel de riesgo: bajo, moderado y alto respectivamente.

- Determinar el valor de tolerancia, sabiendo el nivel de riesgo que afecta a los activos de los procesos comerciales, que puede ser intolerable, tolerable y aceptable (Table N° 28).

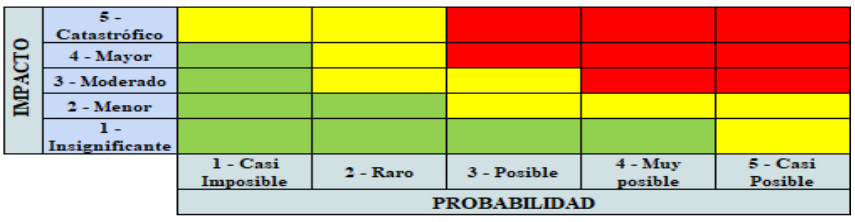


Figura 15: Mapa de Calor
Fuente: Elaboración Propia

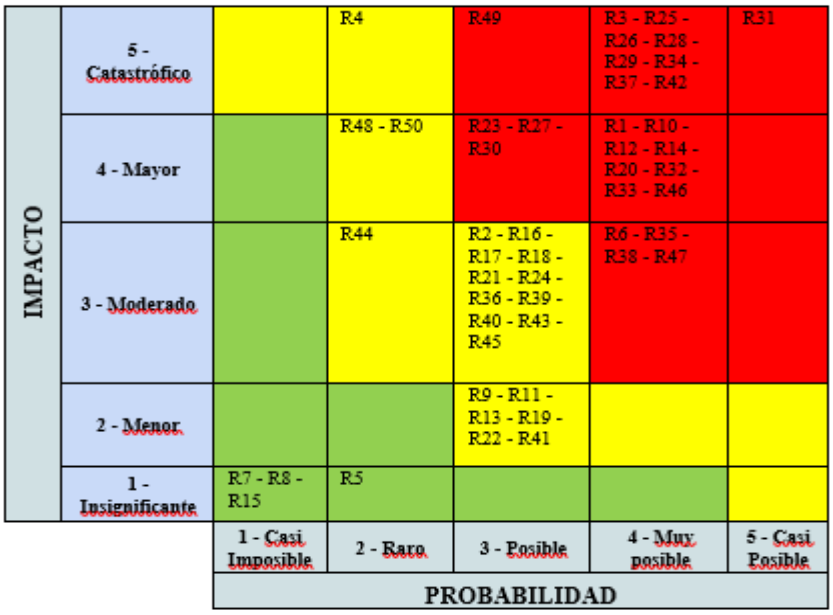


Figura 16: Ejemplo de mapa de calor

VALORACIÓN DE TOLERANCIA	
NIVEL DEL RIESGO	**DESCRICPIÓN**
Alto	Intolerable
Moderado	Tolerable
Bajo	Aceptable

Tabla 28: Valoración de Tolerancia
Fuente: Elaboración Propia

LOGO	**MATRIZ DE VALORIZACIÓN DEL RIESGO**					**Fecha: / /**
	Objetivo: Indicar una breve descripción sobre el objetivo de la matriz.					
NIVEL DEL RIESGO			**IDENTIFICACIÓN DE ACTIVO**			**VALORIZACIÓN**
CÓDIGO	**NIVEL**		**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	
Código del riesgo.	Indicar el valor de acuerdo a la tabla de nivel de riesgo.	Indicar la descripción del valor del nivel de riesgo.	Indicar la clasificación del activo de TI.	Indicar el código del activo de TI	Indicar el nombre del activo de TI.	Valor de la toleración tabla 38.

Tabla 29: Matriz de valorización del riesgo
Fuente: Elaboración Propia

LOGO	MATRIZ DE VALORIZACIÓN DEL RIESGO					Fecha: / /
	Objetivo: Indicar la valorización de cada activo de TI.					
NIVEL DEL RIESGO			**IDENTIFICACIÓN DE ACTIVO**			**VALORIZACIÓN**
CÓDIGO	**NIVEL**		**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	
R1	3	Alto	Proceso	[P_COM]	Proceso de compras	Intolerable
R2	2	Moderado	Proceso	[P_FAC]	Proceso de facturación	Tolerable
R3	3	Alto	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Intolerable
…	…	…	Proceso	[P_ALM]	Proceso de almacén	…
…	…	…	Proceso	[P_CIC]	Proceso de cierre de caja	…
…	…	…	Proceso	[P_COB]	Proceso de cobranzas	…
			Proceso	[P_TES]	Proceso de tesorería	
			Proceso	[P_CON]	Proceso contable	
			Hardware	[HW_COE]	Computadoras de escritorio	
			Hardware	[HW_COE]	Computadoras de escritorio	
			Hardware	[HW_LAP]	Laptop's	
			Hardware	[HW_LAP]	Laptop's	
			Hardware	[HW_TAB]	Tablet's	
			Hardware	[HW_TAB]	Tablet's	
			Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	

Tabla 30: Ejemplo de matriz de valorización del riesgo

Fase IV: Tratamiento del riesgo

En esta fase se debe seleccionar opciones e implementar planes para tratar el riesgo, tomando como punto referencial la información de la matriz de valorización de los riesgos (Tabla N° 17), así como la priorización de los riesgos en el mapa de calor (Figura N° 15), para determinar la estrategia del tratamiento.

4.1. Seleccionar opciones o estrategias para el tratamiento del riesgo

Entrada:

- La matriz de valoración del riesgo (Tabla N° 29).

Salida:

- La matriz de plan de tratamiento de riesgo (Tabla N° 31).

Procedimiento:

- Determinar la estrategia para el tratamiento de cada riesgo identificado en la sub fase de valoración del riesgo. Según el marco de trabajo COBIT, define como posibles estrategias lo siguientes:
  - **Evitar:** suprimir las actividades o las condiciones que generen el riesgo.
  - **Transferir-Compartir:** minimizar la frecuencia y el impacto al transferir o compartir el riesgo. Suele incluirse mediante la contratación de seguro, la tercerización de servicios o instrumentos de mercado de capital a largo plazo. La organización sigue siendo propietaria del riesgo.
  - **Mitigar:** Ejecutar acciones para reducir el impacto y frecuencia de un riesgo. Es necesario implementar procesos de gestión de riesgos que incorpore, elimine o

modifique controles que ocasionen que el riesgo residual pueda ser reevaluado como aceptable.

- ❖ **Aceptar:** Se cuenta con información de sustento acerca del riesgo y se distingue la exposición a la pérdida; sin embargo, no realizan acciones referentes a un riesgo en particular. La organización da por aceptada la pérdida en caso de ocurrencia.

4.2. Preparación e implementación de los planes de tratamiento del riesgo

Los planes de tratamiento del riesgo deben especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado.

Entrada:

- La matriz de valoración del riesgo (Tabla N° 29).

Salida:

- La matriz de plan de tratamiento de riesgo (Tabla N° 31).

Procedimiento:

- Para realizar el tratamiento adecuado de riesgos, se debe revisar cada uno de los activos y sus amenazas identificadas en la fase III, además se debe proponer acciones que permitan implementar una estrategia de respuesta al riesgo para reducir la probabilidad de ocurrencia o el impacto sobre los procesos de comerciales.
- La prioridad será el tratamiento de los riesgos que presenten un nivel alto, sin embargo, se podrán establecer planes de acción para riesgos de menor nivel, si se requiere reducir el nivel del riesgo.

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	Indicar el código del plan.
Nombre:	Nombre del plan.
Estrategia:	◯ Aceptar ◯ Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
Indicar el código y nombre del activo afectado.	
Riesgos a Tratar	
Indicar el riesgo a tratar.	
Objetivo	
Describir el objetivo del plan.	
Área Responsible	
Indicar el área responsable del plan.	
Recursos	
Recursos requeridos para el plan.	
Duración	
Duración del desarrollo del plan.	
Presupuesto	
Monto presupuestado.	

Tabla 31: Matriz de plan de tratamiento de riesgo
Fuente: Elaboración Propia

Fase V: Seguimiento y revisión

En esta fase se debe realizar el seguimiento continuo y revisión periódica del proceso de la gestión del riesgo. Sus resultados serán una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

Entrada:

- La matriz de plan de tratamiento de riesgo (Tabla N° 31).

Salida:

- La matriz de seguimiento y revisión de plan (Tabla N° 32).

Procedimiento:

- Realizar el seguimiento permanente y revisión constante del plan de tratamiento para cada riesgo.

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN	
Código:	Indicar el código del plan.
Nombre:	Nombre del plan.
Estrategia:	◯ Aceptar ◯ Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
Indicar el código y nombre del activo afectado.	
Riesgos a Tratar	
Indicar el riesgo a tratar.	
Objetivo	
Describir el objetivo del plan.	
Área Responsible	
Indicar el área responsable del plan.	
Recursos	
Recursos requeridos para el plan.	

<table>
<tr><td colspan="4">Duración</td></tr>
<tr><td colspan="4">Duración del desarrollo del plan.</td></tr>
<tr><td colspan="4">Presupuesto</td></tr>
<tr><td colspan="4">Monto presupuestado.</td></tr>
<tr><td colspan="4">SEGUIMIENTO Y REVISIÓN</td></tr>
<tr><td>Responsable:</td><td colspan="3">Indicar el área responsable del seguimiento y revisión del plan.</td></tr>
<tr><td>Porcentaje de Cumpliento:</td><td>Indicar el porcentaje de cumplimiento del plan.</td><td>Estado:</td><td>Indicar el estado del plan.</td></tr>
<tr><td>Resultados Esperados del Plan:</td><td colspan="3">Análisis de los resultados esperados de la ejecución del plan.</td></tr>
</table>

Tabla 32: Matriz de seguimiento y revisión de plan
Fuente: Elaboración Propia

3.5. Discusión

- Se consideró identificar metodologías, estándares y marcos de trabajo vinculados con la gestión de riesgos de TI, tales como la ISO 31000, ISO 27005, Cobit 5 para riesgos, Margerit V3.0 y Octave, para luego realizar un cuadro comparativo (ver Anexo 05) tomando como eje principal la ISO 31000 y la relación existente entre los estándares y metodologías antes mencionadas, identificando las fases coincidentes y aportaciones en gestión de riesgos que mejor se adapten a las necesidades de las empresas en estudio donde finalmente se propuso un modelo de gestión de TI para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque, del mismo modo que en la investigación realizada por Murillo y Rivas [9], coincidiendo en el uso de la ISO 31000 para la gestión de riesgos.

- El propósito a nivel general en esta investigación es dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque. Para alcanzar el objetivo principal, se ha validado el modelo con los siguientes instrumentos:
    - El modelo propuesto fue validado a través del juicio de tres profesionales expertos, quienes aprobaron la estructura y el contenido del modelo propuesto en la presente investigación, obteniéndose la aceptación del mismo (ver Anexo 10). Para la medición del nivel de confiabilidad del modelo propuesto entre los profesionales expertos, se aplicó el coeficiente de medición Alfa de Cronbach, donde se obtuvo un 83% de nivel de confiabilidad. Los resultados se muestran a continuación:

Estadísticas de Confiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0.838	0.838	14

Según George y Mallery [31], para determinar los niveles de aceptabilidad para el coeficiente del Alfa de Cronbach son los siguientes:

Intervalo al que pertenece el Coeficiente Alfa	**Valoración de Confiabilidad**
Entre 0.95 y 0.9	Excelente
Entre 0.9 y 0.8	Bueno
Entre 0.8 y 0.7	Aceptable

Entre 0.7 y 0.6	Débil
Entre 0.6 y 0.5	Pobre
Menor a 0.5	Inaceptable

Tomando en cuenta el coeficiente obtenido para elementos estandarizados de 0.838, se concluye que la valoración de confiabilidad del modelo propuesto es Bueno.

- Así mismo para hallar el nivel de concordancia entre los expertos, se usó el coeficiente de Concordancia de Kendall (W), Debido a que el coeficiente puede variar entre 0 y 1 se plantean dos hipótesis:

  - Siendo la hipótesis nula no existe concordancia entre los expertos (W = 0).

  - La hipótesis alterna afirma que existe una concordancia entre los expertos (W > 0).

  Mediante la herramienta SPSS se pudo constatar la concordancia de las evaluaciones dadas por los expertos, teniendo estos resultados:

Estadísticos de prueba	
N	14
W de Kendall	0,321
Chi-cuadrado	9,000
gl (grados de libertad)	2
Sig. (valor de probabilidad)	0,011

De acuerdo al resultado obtenido se acepta la hipótesis alterna es decir existe una concordancia entre las

opiniones de los tres profesionales expertos y que este valor es significativo ($p = 0.011 < 0.05$).

- Con la ejecución del modelo propuesto que se aplicó al caso de estudio, se identificaron 30 activos que intervienen en los procesos comerciales, los mismos que se detallan en la Matriz de Identificación de Activos de TI (Ver Anexo 8), lográndose identificar 50 riesgos, de los cuales 25 contaban con un nivel alto, 21 con nivel moderado y 04 con nivel bajo, los cuales afectan la operación de los procesos comerciales soportados por TI, donde se propusieron 12 planes de tratamiento para los riesgos con nivel alto.

CAPÍTULO IV CONCLUSIONES

- ✓ Se identificaron las metodologías, estándares y normas vigentes de gestión de riesgos de TI, a través de un análisis, comparación y armonización, el cual permitió alinear un modelo de gestión de riesgos adaptado a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque.

- ✓ Se desarrolló el modelo propuesto de gestión de riesgos de TI para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque, el cual consta de 5 fases que permiten realizar como punto inicial la definición del alcance de la gestión de riesgos, comprendidos en el contexto interno y externo en que opera la organización, asimismo permite identificar los procesos que apoyan la estrategia comercial y analizan las actividades que se desarrollan en los procesos comerciales de la organización. También se realiza la identificación, análisis y valoración de escenarios de riesgos que afrontan los activos de TI que dan soporte a los procesos comerciales y que afectan a la organización en el logro de sus objetivos; además el modelo permite proponer opciones y planes de tratamiento para mitigar

los riesgos que no son aceptados por la organización. Finalmente se da seguimiento continuo y revisión periódica a los planes de tratamiento de los escenarios de riesgos.

- ✓ Se validó el modelo propuesto de gestión de riesgos de TI a través de tres profesionales expertos, obteniendo la aceptación del mismo, lo que certifica que el modelo tiene validez para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque. Se utilizó el coeficiente de Alfa de Cronbach para medir su nivel de confiabilidad, donde se obtuvo un valor de 83%, lo que significa, que la confiabilidad del modelo es bueno, también se comprobó el nivel de concordancia entre los expertos, para lo cual se usó el coeficiente de concordancia de Kendall, obteniendo un valor inferior al 0.05, lo que significa, que existe concordancia entre las opiniones de los expertos.

- ✓ Se validó la utilidad del modelo propuesto aplicado al caso de estudio, a través un cuestionario (Ver Anexo 11) aplicado al Jefe de TI, aceptando en un 100% el modelo propuesto, permitiéndole proponer planes de tratamiento adecuados para atenuar el riesgo existente en los procesos comerciales.

REFERENCIAS BIBLIOGRÁFICAS

[1] B. Margarita, «Administración De Riesgos Tecnológicos.,» 29 Octubre 2015. Disponible en: https://margaritaberdugo.wordpress.com/2015/10/29/administracion-de-riesgos-tecnologicos/. [Último acceso: 8 Junio 2020].

[2] E. Comercio, «Whatsapp sufre una caída mundial basada en un profundo cambio,» 4 Mayo 2017. Disponible en: http://www.elcomercio.es/tecnologia/201705/04/whatsapp-caida-mundial-basada-20170504043123.html. [Último acceso: 8 Junio 2020].

[3] Deloitte, «Lecciones tras la caída de Whatsapp,» 2017. Disponible en: https://www2.deloitte.com/do/es/pages/risk/articles/lecciones-tras-la-caida-de-whatsapp.html. [Último acceso: 8 Junio 2020].

[4] C. Baraniuk, «Miles de pasajeros de Delta retrasados por error informático,» 8 Agosto 2016. Disponible en: https://bbc.in/2Mfi7mx. [Último acceso: 8 Junio 2020].

[5] R. Noticias, «Caída del sistema genera aglomeración de pasajeros en el Jorge Chávez,» 22 Mayo 2014. Disponible en: http://rpp.pe/lima/actualidad/caida-de-sistema-genera-aglomeracion-de-pasajeros-en-el-jorge-chavez-noticia-694161. [Último acceso: 8 Junio 2020].

[6] L. República, «Denuncian fallas en el sistema informático de la Sunat,» 23 Junio 2019. Disponible en: https://larepublica.pe/economia/2019/06/22/sunat-denuncian-colapso-de-sistema-informatico/. [Último acceso: 5 Junio 2020].

[7] R. Noticias, «Indecopi multó a Interbank con S/ 76,950 por caída de sistema,» 21 Agosto 2017. Disponible en: https://rpp.pe/economia/economia/indecopi-multo-a-interbank-con-s-76950-por-caida-de-sistema-noticia-1071610. [Último acceso: 8 Junio 2020].

[8] R. Noticias, «Chiclayo: Incendio en empresa Telefónica deja sin señal a miles de usuarios,» 19 Junio 2020. Disponible en: https://rpp.pe/peru/lambayeque/chiclayo-incendio-en-empresa-telefonica-deja-sin-senal-a-miles-de-usuarios-video-noticia-1274345?ref=rpp. [Último acceso: 6 Julio 2020].

[9] M. C. y. S. Rivas, «Propuesta metodológica para la gestión del riesgo en microempresas comercializadoras de electrodomésticos basada en los modelos ISO 31000:2011 y OHSAS 18001:2007,» 2015. Disponible en: https://repositorio.escuelaing.edu.co/bitstream/001/226/1/EC-

Especializaci%C3%B3n%20en%20Gestion%20Integrada%20QHSE-1072493699.pdf. [Último acceso: 16 Mayo 2020].

[10] J. C. B. Santisteban, «Modelo basado en metodologías de gestión de riesgos de TI para contribuir en la moejra de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lmabayeque.,» 2019. Disponible en: http://tesis.usat.edu.pe/bitstream/20.500.12423/2159/1/TM_BandaSantistebanJose.pdf. [Último acceso: 16 Abril 2021].

[11] O. Ñ. Campos, «Modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metología Magerit para mejorar la gestión de seguridad de la información en la universidad nacional Toribio Rodriguez de Mendoza - Chachapoyas Perú.,» 2019. Disponible en: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/6110/BC-%204020%20%c3%91A%c3%91EZ%20CAMPOS.pdf?sequence=1&isAllowed=y. [Último acceso: 18 Abril 2021].

[12] R. C. S. C. Acosta, «Modelo de gestión de riesgos de TI para el cumplimiento de las exigencias de la SBS en sector microfinanciero de Chiclayo.,» 2018. Disponible en: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/6116/BC-1957%20SANTA%20CRUZ%20ACOSTA.pdf?sequence=1&isAllowed=y. [Último acceso: 20 Abril 2021].

[13] K. H. Cabello S.D., «Análisis y Gestión de Riesgo en Proyectos Software. Un nuevo modelo integrando la metodología SEI y Magerit,» Abril 2018. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/67916/Documento_completo.pdf-PDFA.pdf?sequence=1. [Último acceso: 16 Mayo 2020].

[14] M. H. H. Mere, «Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones.,» 2019. Disponible en: http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/11225/Huaura_mm.pdf?sequence=1&isAllowed=y. [Último acceso: 26 Abril 2021].

[15] J. N. Ordeñana, «Aplicación de Gestión de Riesgos Tecnológicos basada en la norma ISO/IEC 27005 en el área de Base de Datos y Sistema Operativo de la Dirección de Informática y Sistema de la DGI,» MARZO 2019. Disponible en: https://core.ac.uk/download/pdf/288314661.pdf. [Último acceso: 31 MAYO 2021].

[16] E. R. B. Alvear, «Propuesta de un Plan de Gestión de Riesgos y Gestión Ética para el Departamento de Tecnologías en el Sector Educativo,» 2017. Disponible en:

http://dspace.ucuenca.edu.ec/bitstream/123456789/28522/1/Trabajo%20de%20titulaci%c3%b3n.pdf. [Último acceso: 31 Abril 2021].

[17] E. y. Z. V. Chillogallo, «Elaboración de un Modelo de Gestión de Riesgos de Tecnologías de Información para la Fiscalía General del Estado,» ENERO 2016. Disponible en: https://bibdigital.epn.edu.ec/bitstream/15000/13730/1/CD-6728.pdf. [Último acceso: 31 ABRIL 2021].

[18] Á. T. G. L Romera, «GESTIÓN DE LOS RIESGOS TECNOLÓGICOS,» *RPM-AEMES,* vol. V, nº 1, 2008.

[19] I. 31000:2018(es), «Gestión del riesgo – Directrices - Risk management — Guidelines,» 2018. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es:fig:4. [Último acceso: 18 Mayo 2020].

[20] ISO/IEC, «Information technology - Security techniques - Information security risk management,» 2011.

[21] R. A. R. y. J. A. C. A. S. A. Behnia, «of Information Security Risk Analysis Methods,» *Smart Computing Review,* vol. II, pp. 81-94, 2012.

[22] ISACA, «COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa,» 2012. Disponible en: https://riunet.upv.es/bitstream/handle/10251/72620/MONFORT%20-%20COBIT%205%20y%20el%20Cuadro%20de%20Mando%20Integral%20como%20herramientas%20de%20Gobierno%20de%20TI.pdf?sequence=2. [Último acceso: 19 Mayo 2020].

[23] P. C. G, «Cobit 5 para riesgos. Metodología. Una visión general.,» Disponible en: https://www.academia.edu/37119477/Pablo_Caneo_G._Cobit_5_para_riesgos._Metodolog%C3%ADa._Una_visi%C3%B3n_general. [Último acceso: 19 Mayo 2020].

[24] M. v. 3.0, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» Octubre 2012. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Último acceso: 18 Mayo 2020].

[25] ISACA, «Marco de Riesgo de TI,» 2009. Disponible en: http://www.ucipfg.com/Repositorio/MATI/MATI-01/Unidad4/lecturas/51855611-Risk-IT-Framework-Espanol.pdf. [Último acceso: 18 Mayo 2020].

[26] C. S. D. I. T. L. Guide for conducting risk assessment, «EEUU NIST, National Institute of Standards and Technology,» Setiembre 2012. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. [Último acceso: 18 Mayo 2020].

[27] S. Amador Donado, «Gestión del riesgo con base en ISO27005 adaptando OCTAVE-S,» 14 Diciembre 2014. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/4737/AMADOR%20DONADO%2c%20SILER.pdf?sequence=1&isAllowed=y. [Último acceso: 4 Mayo 2021].

[28] ¿. e. l. g. d. c. y. c. a. a. t. empresa?, «Aplicaciones y Tecnología del Grupo MALO,» Disponible en: https://aplicacionesytecnologia.com/gestion-de-compras/. [Último acceso: 30 04 2021].

[29] A. I. B. Boubeta, Distribución logística y comercial: La logística en la empresa, España: Ideaspropias Editorial, 2007.

[30] J. L. B. G. y. A. S. Andrés, Cómo mejorar el funcionamiento de la fuerza de ventas (Edirectivos: Marketing), España: Especial Directivos, 2007.

[31] D. Frias Navarro, «Apuntes de Consistencia Interna de las Puntuaciones de un Instrumento de Medida,» Universidad de Valencia, 2021. Disponible en: https://www.uv.es/friasnav/AlfaCronbach.pdf. [Último acceso: 8 Junio 2021].

ANEXOS

Anexo 1: Cuadro Comparativo de Empresas de Ventas de Materiales de Construcción de la Región Lambayeque

CUADRO COMPARATIVO DE EMPRESAS DE VENTAS DE MATERIALES DE CONSTRUCCIÓN DE LA REGIÓN LAMBAYEQUE

DATOS	EMPRESA 01	EMPRESA 02	EMPRESA 03	EMPRESA 04
SECTOR	Ventas de materiales construcción	Ventas de materiales construcción	Ventas de materiales construcción	Ventas de materiales construcción
MISIÓN	Nos esforzamos por satisfacer las necesidades del cliente con productos al mejor precio junto con un servicio de alta calidad, con el compromiso de nuestros socios estratégicos; aplicando los valores de responsabilidad, confianza y honestidad.	Brindar la más variada gama de productos al mercado metal mecánico y de obra gris con un excelente servicio y atención al cliente, manteniendo a nuestros colaboradores motivados.	Somos una empresa dedicada a la comercialización a gran escala de productos ferreteros, eléctricos y plomería; para el hogar y la construcción; ofreciendo la mejor variedad, relación precio-calidad, tiempo de entrega, atención personalizada, superando sus expectativas en el servicio y enfocados a la plena satisfacción de nuestros clientes, distribuidores y profesionales de la construcción.	Brindar al cliente un producto en el costo y en los plazos previstos, ofreciendo calidad en nuestros productos y en la atención, consolidando en estos valores agregados nuestra identidad empresarial a favor del desarrollo del sector de la construcción en nuestra región
VISIÓN	Ser reconocida nacionalmente en la comercializando materiales de construcción, prometiendo atención personalizada a cada uno de nuestros clientes.	Ser la cadena comercial de tiendas con mayor cobertura del mercado metal mecánico y de obra gris en el país.	Ser la mejor opción para nuestros clientes a nivel nacional, aplicando los principios establecidos en nuestra misión. Ser una empresa rentable, y que mediante un crecimiento sostenido y planeado con mayores volúmenes comercializados transfiera beneficios a nuestros clientes, proveedores y empleados.	Constituirse en el líder corporativo en la venta de materiales de construcción en el norte del Perú, a través de su permanente búsqueda de la excelencia en la atención al cliente y su aporte en el desarrollo del sector de la construcción.

VALORES	• Responsabilidad. • Confianza. • Honestidad.	• Vocación de Servicio. • Innovación. • Compromiso. • Trabajo en Equipo. • Honestidad. • Respeto.	• Responsabilidad. • Compromiso. • Trabajo en Equipo. • Respeto.	• Trabajo en Equipo. • Puntualidad. • Respeto. • Responsabilidad.
OBJETIVOS ESTRATÉGICOS	• Maximizar las ventas de las familias de productos. • Segmentación de clientes para ampliar y consolidar los canales de venta.	• Productos de calidad superior a los de nuestros competidores. • Crecer geográficamente que nuestros competidores.	• Tener participación en el mercado lambayecano. • Costos más bajos que nuestros competidores.	• Brindar un servicio de calidad a nuestros clientes. • Ampliar línea de productos al costo más bajo.
DESCRIPCIÓN DEL ÁREA DE TI	Depende de la Gerencia de General, conformado por 5 personas (1 Jefe de TI, 2 Analista de TI y 2 de soporte técnico).	Depende de la Gerencia General, conformado por 5 personas, divididos en 4 sub áreas como son desarrollo, producción, mesa de ayuda y soporte.	Depende de la Gerencia General conformado por 2 personas (1 Jefe TI y 1 Soporte de TI).	Depende de la Gerencia General conformado por 3 personas, divididos en 2 áreas como son jefatura de TI y desarrollo y/o soporte de TI.

Anexo 2: Cuestionario de Diagnóstico de Gestión de Riesgos de Tecnologías de Información

CUESTIONARIO DE DIAGNÓSTICO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Dirigida: Jefe de TI.

Fecha : _____

Empresa: _____

Nombre : _____

Procedimiento: Se está realizando un estudio acerca de la gestión de riesgos de tecnologías de la información, con la finalidad de identificar el nivel de riesgos de tecnologías de información y como se viene realizando la gestión de los mismo en la empresa donde labora.

La encuesta fue desarrollada teniendo en cuenta el marco COBIT 5.

Indicaciones: Marque con una X la respuesta seleccionada por usted.

N°	PREGUNTA	SI	NO
1	¿Se ha establecido un marco de referencia para la gestión de riesgos de TI en la empresa?		
2	¿Se ha establecido el alcance del análisis de riesgos?		
3	¿Se ha determinado el apetito de riesgo para los riesgos de TI?		
4	¿Existe un área responsable de la gestión de riesgos de TI?		
5	¿La empresa cuenta con un procedimiento o método para identificar, clasificar y analizar los riesgos de TI?		
6	¿La empresa tiene un inventario de los activos relaciones con TI?		
7	¿Se tienen identificados los riesgos a los que están expuestos los activos de la empresa?		
8	¿Se ha identificado y establecido controles clave de mitigación para estos riesgos?		
9	¿Se promueve una cultura de riesgo en la empresa?		
10	¿Los empleados son conscientes de los posibles riesgos de TI?		
11	¿Se mantiene un inventario de actividades de control que estén en marcha para gestionar el riesgo?		
12	¿Se informa de los resultados del análisis de riesgos a todas las partes interesadas?		
13	¿Se ha definido proyectos para reducir el efecto del riesgo actual?		
14	¿El desempeño en la gestión de riesgos de TI se monitorea regularmente?		
15	¿Se ha documentado planes que especifiquen los pasos a seguir cuando un evento de riesgo pueda causar un incidente significativo?		

Anexo 3: Resultado de Cuestionario de Gestión de Riesgos de Tecnologías de Información

RESULTADO DE CUESTIONARIO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN

N°	PREGUNTA	EMPRESA 01	EMPRESA 02	EMPRESA 03	EMPRESA 04
1	¿Se ha establecido un marco de referencia para la gestión de riesgos de TI en la empresa?	NO	NO	NO	SI
2	¿Se ha establecido el alcance del análisis de riesgos?	NO	SI	NO	SI
3	¿Se ha determinado el apetito de riesgo para los riesgos de TI?	NO	SI	NO	NO
4	¿Existe un área responsable de la gestión de riesgos de TI?	NO	NO	NO	NO
5	¿La empresa cuenta con un procedimiento o método para identificar, clasificar y analizar los riesgos de TI?	SI	NO	SI	SI
6	¿La empresa tiene un inventario de los activos relaciones con TI?	SI	SI	SI	SI
7	¿Se tienen identificados los riesgos a los que están expuestos los activos de la empresa?	NO	SI	SI	NO
8	¿Se ha identificado y establecido controles clave de mitigación para estos riesgos?	SI	NO	SI	SI
9	¿Se promueve una cultura de riesgo en la empresa?	NO	NO	SI	NO
10	¿Los empleados son conscientes de los posibles riesgos de TI?	NO	SI	SI	NO
11	¿Se mantiene un inventario de actividades de control que estén en marcha para gestionar el riesgo?	NO	SI	SI	NO
12	¿Se informa de los resultados del análisis de riesgos a todas las partes interesadas?	NO	SI	NO	NO
13	¿Se ha definido proyectos para reducir el efecto del riesgo actual?	NO	NO	SI	NO
14	¿El desempeño en la gestión de riesgos de TI se monitorea regularmente?	NO	NO	SI	NO
15	¿Se ha documentado planes que especifiquen los pasos a seguir cuando un evento de riesgo pueda causar un incidente significativo?	NO	NO	NO	NO

Anexo 4: Gráficos de los Resultados del Cuestionario

GRÁFICOS DE LOS RESULTADOS DEL CUESTIONARIO

Gráfico 1: ¿Se ha establecido un marco de referencia para la gestión de riesgos de TI en la empresa?

Gráfico 2: ¿Se ha establecido el alcance del análisis de riesgos?

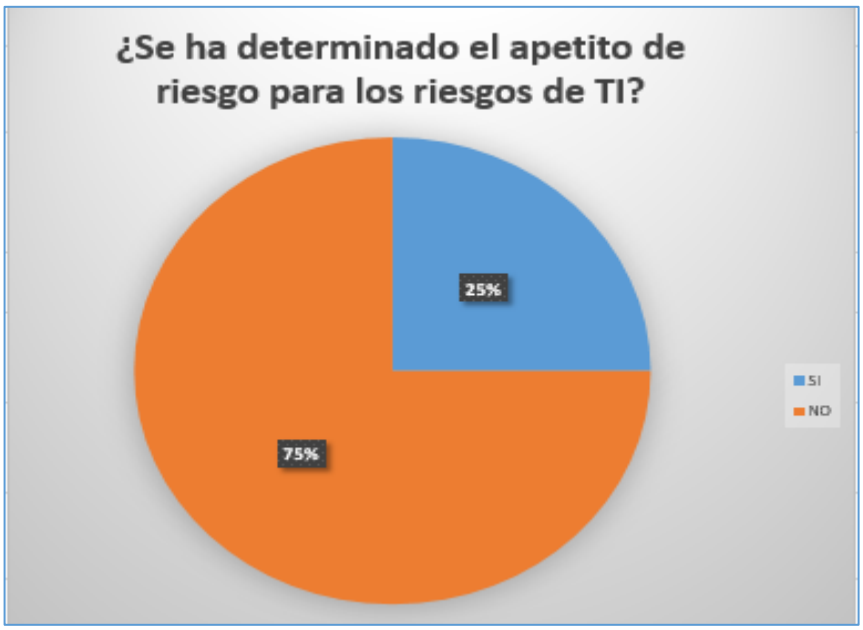


Gráfico 3: ¿Se ha determinado el apetito de riesgo para los riesgos de TI?

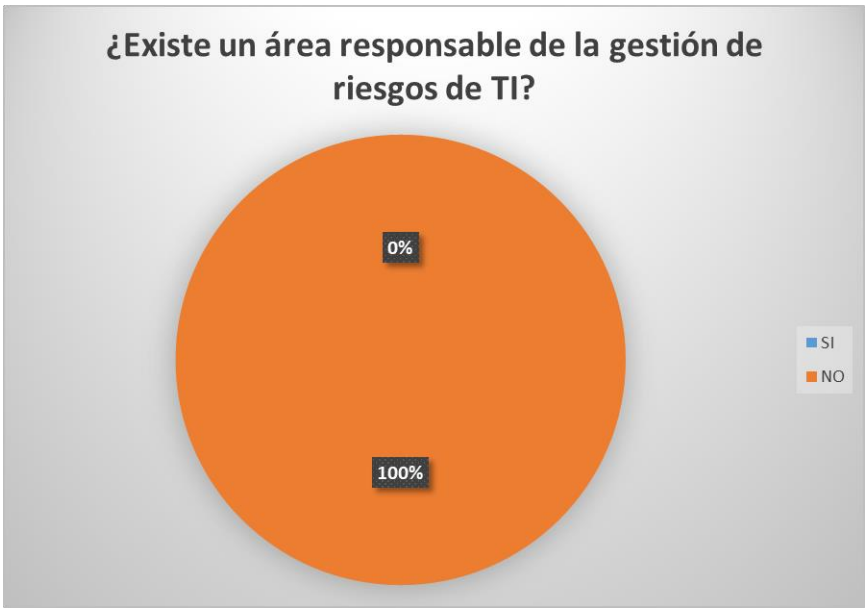


Gráfico 4: ¿Existe un área responsable de la gestión de riesgos de TI?

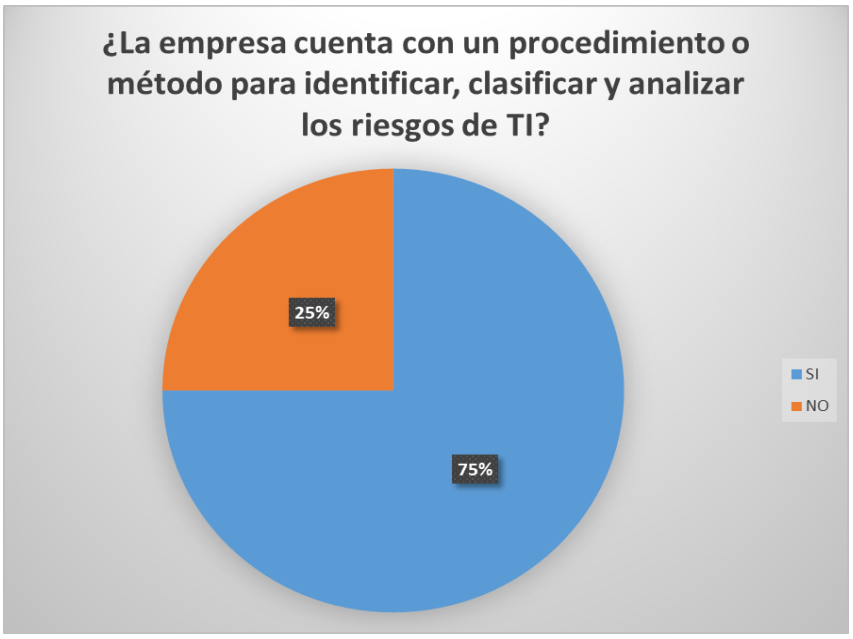


Gráfico 5: ¿La empresa cuenta con un procedimiento o método para identificar, clasificar y analizar los riesgos de TI?

Gráfico 6: ¿La empresa tiene un inventario de los activos relaciones con TI?

Gráfico 7: ¿Se tienen identificados los riesgos a los que están expuestos los activos de la empresa?

Gráfico 8: ¿Se ha identificado y establecido controles clave de mitigación para estos riesgos?

Gráfico 9: ¿Se promueve una cultura de riesgo en la empresa?

Gráfico 10: ¿Los empleados son conscientes de los posibles riesgos de TI?

Gráfico 11: ¿Se mantiene un inventario de actividades de control que estén en marcha para gestionar el riesgo?

Gráfico 12: ¿Se informa de los resultados del análisis de riesgos a todas las partes interesadas?

Gráfico 13: ¿Se ha definido proyectos para reducir el efecto del riesgo actual?

Gráfico 14: ¿El desempeño en la gestión de riesgos de TI se monitorea regularmente?

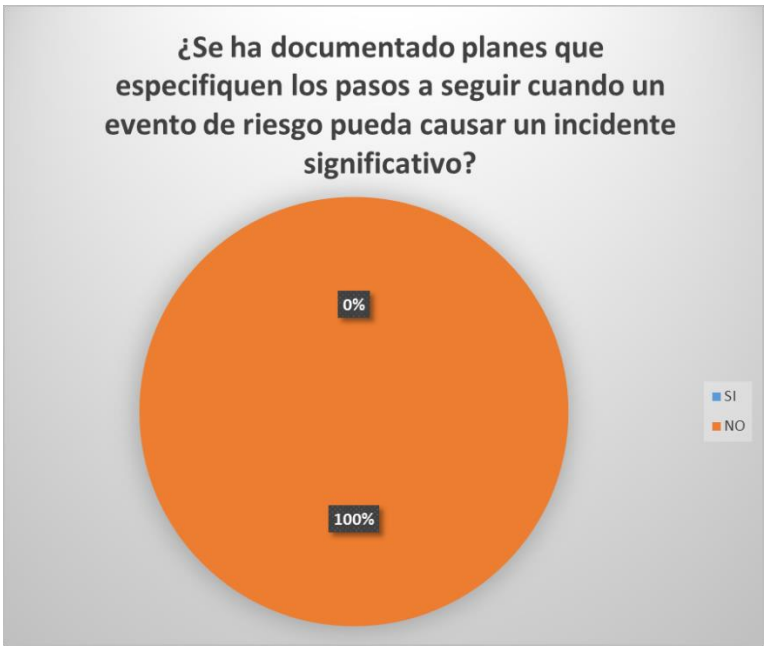


Gráfico 15: ¿Se ha documentado planes que especifiquen los pasos a seguir cuando un evento de riesgo pueda causar un incidente significativo?

Anexo 5: Cuadro de Análisis de Estándares, Marcos de Trabajo y Metodologías

CUADRO DE ANÁLISIS DE ESTÁNDARES, MARCOS DE TRABAJO Y METODOLOGÍAS

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
Proporciona directrices para gestionar los riesgos en las organizaciones		Proporciona guías para la gestión de los riesgos de seguridad de la información en las organizaciones.		Ayuda a las organizaciones a crear valor desde TI y optimizando los niveles de riesgo y uso de recursos	Metodología de análisis y gestión de riesgos de los sistemas de información		Metodología de análisis de riesgos, estudia los riesgos en base a tres principios Confidencialidad, Integridad y Disponibilidad.	
Fase 1: Alcance, contexto, criterios	**- Definición del alcance:** La organización debería definir el alcance de sus actividades de gestión de riesgos.	**Fase 1: Establecimiento del contexto**	**- Definir alcance y límites:** El alcance debería definirse para asegurar que todos los activos relevantes son tomados en cuenta en la evaluación del riesgo, identificando límites para abordar aquellos riesgos que surjan a través de estos límites.	- El dominio gobierno del riesgo asegura que el enfoque adoptado de gestión de riesgos sea adecuado para la situación de la organización.	**Fase 1: Método de análisis de riesgos**	- Determinar el alcance del proyecto. Resultado: Perfil de proyecto de análisis de riesgo. - Planificación del proyecto. Resultado: Plan de trabajo y procedimientos. - Lanzamiento del proyecto. Resultados: Cuestionario para	**Fase 1: Visión Organizativa**	- Definir activos. - Definir amenazas. - Definir vulnerabilidades. - Definir requerimientos de seguridad.
	- Establecer el contexto interno e externo: Son el entorno en el cual la organización busca definir y lograr sus objetivos.		**- Establecimiento del contexto:** El contexto externo e interno para la gestion de riesgo de la seguridad de la información debe ser establecido.	- Incluye prácticas de gestión para entender el contexto interno e externo.				

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
	- Definir los criterios de riesgo: La organización debería precisar la cantidad y el tipo de riesgo que puede o no pueda tomar, con relación a los objetivos, así como definir los criterios para valorar la importancia del riesgo.		**- Criterio Básico:** Se debe definir criterios de evaluación del riesgo, impacto y aceptación del riesgo.	- Provee una guía a las empresas para desarrollar criterios de riesgos específicos, y así definir el impacto en el negocio, establecer el apetito de riesgo, límites de tolerancia y agregación del riesgo.		entrevistas, catálogo de tipo de activos, la relación de dimensiones de seguridad, criterios de valoración.		
			- Organización para la gestión de riesgos de seguridad de la información: La organización y las responsabilidades para el proceso de gestión de riesgos de seguridad de la información deben ser establecidos y mantenidos.					

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
Fase 2: Evaluación del riesgo	**- Identificación de los riesgos:** El propósito es encontrar , reconocer y describir los riesgos que puedan ayudar o impedir a una organización lograr sus objetivos.	**Fase 2: Valoración del riesgo**	**- Identificación del riesgo:** • Identificación de los activos. • Identificación de las amenazas. • Identificación de los controles existentes. • Identificaciones de las vulnerabilidades. • Identificación de las consecuencias.	- Incluye prácticas de gestión para identificar el riesgo asociado con los servicios y productos de la organización que dependen de TI y a identificar los factores de riesgo que contribuyen a eventos e incidentes ocurridos en la organización.	**Fase 2: Análisis de riesgo**	**- Caracterización de los activos:** Determinar los activos relevantes para la organización, su interrelación y su valor. - **Caracterización de las amenazas:** Determinar a qué amenazas están expuestos aquellos activos. - **Caracterización de las salvaguardas:** Determinar que salvaguardas		
	- Análisis de los riesgos: El propósito es comprender la naturaleza del riesgo y sus características, identificando la causa y las fuentes del riesgo, su impacto positivo y negativo y la probabilidad de ocurrencia.		**- Análisis del riesgo:** • Metodología de análisis del riesgo. • Evaluación de las consecuencias. • Evaluación de la probabilidad de incidentes. • Determinación del nivel de riesgo.	- El análisis del riesgo es el proceso por el cual son estimados la frecuencia y el impacto de los escenarios de riesgo de TI.			**Fase 2: Visión Tecnológica**	- Definir componentes claves. - Vulnerabilidades técnicas.

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
	- Valoración de los riesgos: El propósito de la valoración es apoyar a la toma de decisiones.		**Evaluación del riesgo:** El nivel de los riesgos debe ser comparado contra los criterios de evaluación de riesgos y el criterio de aceptación de riesgo.	Aborda esta fase del proceso en forma intrínseca.		hay dispuestas y cuán eficaces son frente al riesgo. - **Estimación del estado de riesgo:** Consta de dos actividades: • Estimación del impacto. • Estimación del riesgo.	**Fase 3: Estrategia y Desarrollo del Plan**	- Identificar riesgos. - Identificar estrategias de protección. - Establecer planes de mitigación.
Fase 3: Tratamiento de los riesgos	**- Selección de las opciones para el tratamiento del riesgo:** Implica hacer un balance entre los beneficios potenciales derivados del logro de los objetivos como costos, esfuerzo o desventajas de la implementación.	**Fase 3: Tratamiento del riesgo**	- Reducir el riesgo. - Evitar el riesgo. - Transferir el riesgo.	- Incluye una guía de las opciones de respuesta comunes y cómo se aplican a un contexto de TI.	**Fase 3: Gestión de Riesgos**	- Identificación de proyectos de seguridad. - Planificación de los proyectos de seguridad. - Ejecución del plan.		

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
	- Preparación e implementación de los planes de tratamiento del riesgo: Su propósito es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento. El plan de tratamiento debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implementar.			- Define respuestas especificas a riesgos para abordar diferentes tratamientos para los riesgos. - Utiliza el desarrollo de escenarios para la identificación de riesgos.				
		Fase 4: Aceptación del riesgo	- Convivir con el riesgo.					

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
Fase 4: Seguimiento y revisión	- El propósito es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso.	**Fase 5: Monitoreo y revisión del riesgo**	- Monitoreo y revisión del proceso. - Monitoreo y revisión de los factores de riesgo. Los riesgos y sus factores (amenazas, vulnerabilidad, probabilidad de ocurrencia, impactos, valor de los activos) deberían ser monitoreados y revisados para identificar cualquier cambio en el contexto de la organización en una etapa temprana, y mantener una vista general del entorno completo de riesgo.	- Incluye metas y métricas que pueden ser utilizados para medir el desempeño, y un modelo de madurez para establecer una hoja de ruta para mejorar el proceso de gestión de riesgos.				

ISO 31000:2018		ISO 27005		COBIT 5 para Riesgo	MAGERIT V3.0		OCTAVE	
Fase 5: Comunicación y consulta	- El propósito es asistir a las partes pertinentes a comprender el riesgo y planificar la comunicación interna y externa.	**Fase 6: Comunicación del riesgo**	- La información acerca del riesgo debería ser intercambiada o compartida entre las personas que toman las decisiones y otras partes interesadas.	- El habilitador "información" incluye información específica a ser comunicada entre las partes interesadas.				
Fase 6: Registro e informe	- El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados.			- Incluye prácticas de gestión para rastrear decisiones de riesgos claves y especifica entradas y salidas para estas prácticas de gestión.				

Anexo 6: Descripción de Análisis de Estándares, Marcos de Trabajo y Metodologías

Fase I: Alcance, contexto y criterios

Según ISO 31000, está fase tiene como propósito adaptar el proceso de gestión de riesgo, permitiendo una evaluación de riesgos eficazmente y un tratamiento apropiado de riesgo.

<table>
<tr><th colspan="2">ISO 31000:2018</th><th colspan="3">ISO 27005:2011</th><th>MAGERIT V3.0</th></tr>
<tr><td rowspan="4">Alcance, contexto y criterios</td><td>Definir el alcance</td><td rowspan="4">Establecimiento del contexto</td><td>Alcance y limites</td><td>-</td><td>-</td></tr>
<tr><td>Contexto externo e interno</td><td>Contexto externo e interno</td><td>-</td><td>Contexto</td></tr>
<tr><td rowspan="3">Definir criterios del riesgo</td><td rowspan="3">Criterios básicos</td><td>Criterios de evaluación</td><td rowspan="3">Criterios</td></tr>
<tr><td>Criterios de impacto</td></tr>
<tr><td>Criterios de aceptación</td></tr>
</table>

1.1. Definición del alcance

Según ISO 31000, la organización deberá definir el alcance de sus actividades de gestión de riesgo, los objetivos y el alineamiento de los objetivos de la organización.

ISO 31000:2018	ISO 27005:2011
• Objetivos y decisiones que necesitan ser tomadas. • Resultados esperados de los pasos a ser seguidos en el proceso. • Tiempo, ubicación, inclusiones y exclusiones específicas. • Herramientas y técnicas de evaluación del riesgo apropiadas. • Recursos requeridos, responsabilidades y registros a ser mantenidos. • Relaciones con otros proyectos, procesos y actividades.	**Estudio de la organización** • Propósito principal. • Negocio. • Misión. • Valores. • Estructura. • Organigrama. • Objetivos estratégicos. **Restricciones que afectan a la organización** • De carácter político, estratégico, cultural. • Territoriales. • Clima económico y político. • Relativas al personal.

	Restricciones que afectan el alcance • Derivadas de procesos preexistentes. • Técnicas. • Financieras. • Ambientales. • Organizacionales.

1.2. Contexto externo e interno

Según ISO 31000, se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización donde se busca definir y lograr sus objetivos.

- **Contexto externo**

  Según ISO 31000, es el entorno externo que la organización busca lograr sus objetivos.

  Según Magerit, es el entorno externo en el que opera la organización.

ISO 31000:2018	ISO 27005:2011	Magerit v3.0	Cobit 5
• Factores sociales, culturales, políticos, legales, regulatorios, financieros, tecnológicos, económicos y ambientales. • Factores clave y tendencias que afectan los objetivos. • Relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas.	• Entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo. • Factores clave y tendencias que tienen impacto en los objetivos de la organización.	• Cultural • Social • Político • Obligaciones, legales, reglamentarias y contractuales • Competencia	• Factores económicos y de mercado. • Tasa de cambio del mercado/ciclo de vida del producto • Industria y competencia. • Ambiente regulatorio. • Panorama de amenazas.

- **Contexto interno**

  Según ISO 31000, es el entorno interno que la organización busca lograr sus objetivos.

  Según Magerit, el entorno interno son las actividades en la que se desenvuelve la organización.

ISO 31000:2018	ISO 27005:2011	Cobit 5
• Visión, misión y valores. • Gobierno, estructura organizacional, roles y responsabilidades. • Estrategia, objetivos y políticas. • Cultura de la organización. • Las relaciones con las partes interesadas, teniendo en cuenta sus percepciones y valores.	• Gobierno, estructura organizacional, roles y responsabilidades. • Políticas, objetivos y estrategias que existen para alcanzarlos. • Relaciones, percepciones y valores de las partes interesadas internas. • Cultura de la organización.	• Metas y objetivos de la empresa. • Importancia estratégica de TI para la empresa. • Complejidad de TI. • Prioridades estratégicas. • Cultura de la empresa. • Capacidad financiera.

1.3. Definición de los criterios de riesgo

Según ISO 31000, la organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos, así como también debería definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones.

ISO 31000:2018	ISO 27005:2011
• Naturaleza y tipo de incertidumbres que pueden afectar los resultados y objetivos. • Cómo se definirán y medirán las consecuencias y la probabilidad. • Factores relacionados con el tiempo. • Consistencia en el uso de mediciones. • Cómo se determinará el nivel de riesgo. • Cómo se tendrán en cuenta las combinaciones y secuencias de riesgos múltiples. • Capacidad de la organización.	**Criterios de Evaluación** • Valor estratégico del proceso. • Criticidad de los activos de información involucrados. • Requisitos legales y regulatorios. • Importancia operativa y empresarial de la integridad, confidencialidad y disponibilidad. • Expectativas y percepciones de las partes interesadas. • Consecuencias negativas para la reputación. **Criterios de Impacto** • Nivel de clasificación del activo de información afectado. • Incumplimientos de seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad). • Operaciones deterioradas. • Pérdida de valor empresarial y financiero. • Interrupción de planes y fechas límite. • Incumplimientos de requisitos legales, regulatorios. **Criterios de Aceptación** • Pueden expresarse como la relación entre el beneficio estimado y el riesgo estimado. • Pueden aplicarse diferentes criterios a diferentes clases de riesgo. • Pueden incluir requisitos para futuros tratamientos adicionales.

Fase II: Evaluación del riesgo

Según ISO 31000, es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo, de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas.

<table>
<tr><th colspan="2">ISO 31000:2018</th><th colspan="3">ISO 27005:2011</th><th colspan="2">Magerit v3.0</th><th colspan="2">Octave</th></tr>
<tr><td rowspan="4">Evaluación del riesgo</td><td rowspan="2">Identificación del riesgo</td><td rowspan="4">Evaluación del riesgo</td><td rowspan="2">Identificación del riesgo</td><td>Identificación de activos</td><td rowspan="4">Análisis de riesgos</td><td rowspan="4">Caracterización de los activos
▪ Identificación de los activos.
▪ Dependencias entre activos.
Caracterización de las amenazas
▪ Identificación de las amenazas.
Caracterización de las salvaguardas
▪ Identificación de las salvaguardas pertinentes.
Estimación del estado del riesgo
▪ Estimación del impacto.
▪ Estimación del riesgo.</td><td>Visión organizativa</td><td>▪ Definir activos.
▪ Definir amenazas.
▪ Definir vulnerabilidades.
▪ Definir requerimientos de seguridad.</td></tr>
<tr><td>Identificación de amenazas</td></tr>
<tr><td>Identificación de controles existentes</td></tr>
<tr><td>Identificación de vulnerabilidades</td></tr>
<tr><td></td><td></td><td>Identificación de Consecuencias</td><td></td><td></td></tr>
<tr><td></td><td rowspan="3">Análisis del riesgo</td><td rowspan="3">Análisis del riesgo</td><td>Metodologías de análisis de riesgos</td><td rowspan="3">Visión tecnológica</td><td rowspan="3">▪ Definir componentes claves.
▪ Vulnerabilidades técnicas.</td></tr>
<tr><td></td><td>Evaluación de consecuencias</td></tr>
<tr><td></td><td>Evaluación de probabilidad de incidentes</td></tr>
<tr><td></td><td></td><td></td><td>Determinación del nivel de riesgo</td><td></td><td></td></tr>
<tr><td></td><td>Valoración del riesgo</td><td></td><td>Valoración del riesgo</td><td>-</td><td></td><td></td><td></td><td></td></tr>
</table>

2.1. Identificación del riesgo

Según ISO 31000, es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos, para lo cual se debe contar con información pertinente, apropiada y actualizada.

ISO 31000:2018	ISO 27005:2011	Magerit v3.0	Octave
• Fuentes de riesgos tangibles e intangibles. • Amenazas y oportunidades. • Vulnerabilidades y capacidades. • Naturaleza y valor de los activos y recursos.	• Identificación de activos • Valoración de los activos • Identificación de Amenazas y Vulnerabilidades. • Identificación de controles existentes.	• Identificación de activos • Valoración de los activos • Tipos de amenazas (de origen natural, defectos de las aplicaciones, entre otras).	• Identificación de activos (sistemas, información, aplicaciones, personas). • Valoración de los activos (disponibilidad, integridad, confidencialidad).

2.2. Análisis del riesgo

Según ISO 31000, es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo, el cual implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia.

ISO 31000:2018	ISO 27005:2011
• Probabilidad de eventos y consecuencias. • Naturaleza y magnitud de las consecuencias. • Complejidad y conectividad. • Factores relacionados con el tiempo y la volatilidad. • Efectividad de los controles existentes. • Sensibilidad y niveles de confianza.	• Metodologías de Análisis de Riesgos. • Valoración Cualitativa de Activos. • Aspectos para la Valoración de Activos. • Criterios para evaluar las posibles consecuencias. • Evaluación de Probabilidad de Incidentes.

2.3. Valoración del riesgo

Según ISO 31000, es apoyar a la toma de decisiones, el cual comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.

ISO 31000:2018	ISO 27005:2011
• Considerar opciones de tratamiento de riesgo. • Emprender un análisis adicional para comprender mejor el riesgo. • Mantener los controles existentes. • Reconsiderar objetivos. • No hacer nada más.	• Propiedades de seguridad de la información. • Importancia del proceso de negocio o actividad respaldada por un activo o conjunto de activos. • Prioridades para el tratamiento del riesgo. • Si una actividad debe ser emprendida.

Fase III: Tratamiento del riesgo

Según ISO 31000, su propósito es seleccionar e implementar opciones para abordar el riesgo.

<table>
<tr><th colspan="2">ISO 31000:2018</th><th colspan="2">ISO 27005:2011</th><th colspan="2">Magerit v3.0</th><th colspan="2">Cobit 5</th></tr>
<tr><td rowspan="5">Tratamiento de Riesgo</td><td rowspan="4">Selección de las opciones de tratamiento del riesgo.</td><td rowspan="5">Tratamiento de Riesgo</td><td>Modificar el riesgo.</td><td rowspan="5">Decisión de tratamiento</td><td>Eliminación</td><td rowspan="5">Estrategias de tratamiento</td><td>Evitar</td></tr>
<tr><td>Retener el riesgo.</td><td>Mitigación</td><td>Transferir - Compartir</td></tr>
<tr><td>Evitar el riesgo.</td><td>Compartición</td><td>Mitigar</td></tr>
<tr><td>Transferir el riesgo.</td><td>Financiación</td><td>Aceptar</td></tr>
<tr><td>Preparación e implementación de los planes de tratamiento del riesgo.</td><td>-</td><td>-</td><td>-</td></tr>
</table>

3.1. Selección de las opciones para el tratamiento del riesgo

Según el marco de trabajo COBIT, define como posibles estrategias lo siguientes:

- **Evitar:** Dejar de realizar las actividades o las condiciones que generen el riesgo.
- **Transferir-Compartir:** Reducir la frecuencia y el impacto al transferir o compartir el riesgo. Suele darse a través de la contratación de seguro, la externalización de servicios o instrumentos de mercado de capital a largo plazo. La organización sigue siendo propietaria del riesgo.
- **Mitigar:** Ejecutar acciones para reducir la frecuencia e impacto de un riesgo. Implementar procesos de gestión de riesgos para introducir, eliminar, modificar controles que permitan que el riesgo residual puede ser reevaluado como aceptable.

- **Aceptar:** Se cuenta con información de sustento acerca del riesgo y se reconoce la exposición a la pérdida; sin embargo, no se toman acciones relativas a un riesgo en particular. La organización acepta la pérdida en caso ocurra.

3.2. Preparación e implementación de los planes de tratamiento del riesgo

Según ISO 31000, es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado, el cual debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implementar.

Fase IV: Seguimiento y revisión

Según ISO 31000, es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

Según ISO 27005, los riesgos y sus factores (amenazas, vulnerabilidad, probabilidad de ocurrencia, impactos, valor de los activos) deberían ser monitoreados y revisados para identificar cualquier cambio en el contexto de la organización en una etapa temprana, y mantener una vista general del entorno completo de riesgo.

Fase V: Comunicación y consulta

Según ISO 31000, el propósito de la comunicación es promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica

obtener retroalimentación e información para apoyar a la toma de decisiones.

Según ISO 27005, la información acerca del riesgo debería ser intercambiada o compartida entre las personas que toman las decisiones y otras partes interesadas.

Fase VI: Registro e informe

Según ISO 31000, el proceso de la gestión de riesgos y sus resultados se deberían documentar e informar a las partes interesadas, y apoyar a la alta dirección a cumplir sus responsabilidades.

Anexo 7: Estándares, Marcos de Trabajo y Metodologías Utilizadas en el Modelo Propuesto

ESTANDARES, MARCOS DE TRABAJO Y METODOLOGIAS UTILIZADAS EN EL MODELO PROPUESTO		
FASES	**ACTIVIDADES**	**ESTANDAR, MARCO DE TRABAJO Y METODOLOGIA**
FASE I: ALCANCE Y CONTEXTO	1.1. Definir el Alcance	ISO 31000:2018
	1.2. Establecer el Contexto 1.2.1. Contexto Interno - Cultura Organizacional . Misión . Visión . Valores . Partes Interesadas - Estructura Organizacional - Objetivos . Estratégicos . Organizacionales - Recursos 1.2.2. Contexto Externo - Ámbito Sociocultural - Ámbito Económico - Ámbito Competitivo - Ámbito Tecnológico	ISO 31000:2018 ISO 27005:2018
FASE II: PROCESOS COMERCIALES	2.1. Identificar los Procesos Comerciales 2.2. Análisis de los Procesos Comerciales	-
FASE III: EVALUACIÓN DEL RIESGO	3.1. Identificación del riesgo 3.1.1. Identificación de los activos 3.1.2. Valoración de los activos 3.1.3. Identificar las amenazas 3.1.4. Identificar las vulnerabilidades	ISO 31000:2018 MAGERIT V3.0 ISO 27005:2018
	3.2. Análisis del riesgo - Evaluación de la probabilidad de ocurrencia - Evaluación de las consecuencias / impacto - Determinación del nivel de riesgo	ISO 31000:2018 ISO 27005:2018
	3.3. Valoración del riesgo - Priorización del riesgo - Establecer nivel de tolerancia	ISO 31000:2018
FASE IV: TRATAMIENTO DEL RIESGO	4.1. Selección de opciones de tratamiento de riesgo 4.2. Proponer planes de tratamiento de riesgo	ISO 31000:2018 COBIT 5 para Riesgo
FASE V: SEGUIMIENTO Y REVISIÓN	5.1. Seguimiento y Revisión	ISO 31000:2018

Anexo 8: Aplicación del Modelo Propuesto a la Empresa 01

Fase I: Alcance y contexto

1.1. Definir el alcance

- Entrada: Plan estratégico de la empresa 01.
- Técnica utilizada: Lluvia de ideas.
- Herramienta utilizada: Reunión virtual por la plataforma zoom.

LOGO	MATRIZ DE DEFINICIÓN DEL ALCANCE		Fecha: / /
	Objetivo: Definir el alcance de la gestión de riesgos.		
Nro.	**COMPONENTE**	**DESCRIPCIÓN**	
1	**AREA RESPONSABLE DEL COMPONENTE**	Área de Tecnologías de la información y Comunicaciones.	
2	**FECHA**	15 de diciembre del 2020.	
3	**HORA DE INICIO**	10:00 a.m.	
4	**HORA DE FIN**	11:45 a.m.	
5	**TIPO DE TECNICA A UTILIZAR**	(x) Reunión Virtual, indicar plataforma: ZOOM.	
		( ) Reunión Presencial, indicar el lugar: _____.	
6	**PARTICIPANTES**	Gerencia General.	
		Gerencia de Administración y Finanzas.	
		Gerencia Comercial.	
		Jefes de Ventas.	
		Jefes Administrativos.	
		Jefes de Tecnologías de la Información y Comunicaciones.	
		Jefe de Contabilidad.	
		Jefe de Tesorería.	
		Jefe de Almacén.	
7	**OBJETIVOS**	Desarrollar una cultura de gestión de riesgos.	
		Realizar la identificación, análisis y valoración de los riesgos de los activos de TI, que dan soporte a los procesos comerciales de la organización.	
		Identificar amenazas y reducir vulnerabilidades presentadas en los activos de TI.	
8	**ALCANCE**	El procedimiento es aplicable para dar soporte a los procesos comerciales de la organización.	

1.2. Establecer el contexto

1.2.1. Contexto interno

- Entrada: Plan estratégico, manual de organización y funciones, organigrama y el inventario de activos de la empresa 01.
- Técnica utilizada: Lluvia de ideas.
- Herramienta utilizada: Reunión virtual por la plataforma zoom.

LOGO	MATRIZ DE CONTEXTO INTERNO	Fecha: / /
	Objetivo: Establecer el contexto interno de la organización.	

❖ **Cultura organizacional**

- **Misión**

  Nos esforzamos por satisfacer las necesidades del cliente con productos al mejor precio junto con un servicio de alta calidad, con el compromiso de nuestros socios estratégicos; aplicando los valores de responsabilidad, confianza y honestidad.

- **Visión**

  Ser reconocida nacionalmente comercializando materiales de construcción, prometiendo atención personalizada a cada uno de nuestros clientes.

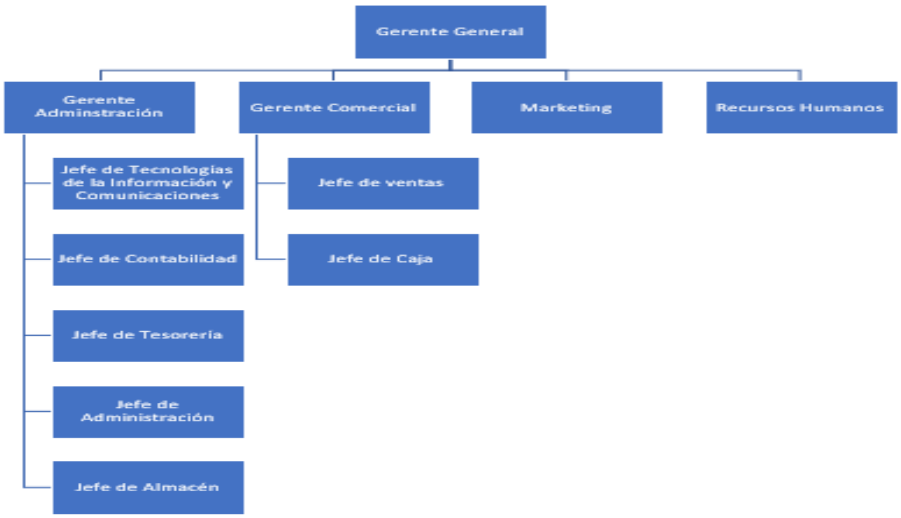
- **Valores**

  Responsabilidad, confianza y honestidad

- **Partes Interesadas**

  Personal de gerencia, personal administrativo, personal comercial, socios estratégicos.

❖ **Estructura Organizacional**



LOGO	MATRIZ DE CONTEXTO INTERNO	Fecha: / /
	Objetivo: Establecer el contexto interno de la organización.	

❖ **Objetivos Organizacionales**

- **Estratégico**
  - Ampliar los actuales mercados.
  - Ampliar la cartera de clientes a nivel nacional.
  - Promover el desarrollo humano.
  - Gestionar estrategias para desarrollar proveedores comprometidos.
  - Mejorar y optimizar los procesos.
- **Organizacional**

  Consolidar el liderazgo de la organización en el mercado de venta de materiales de construcción, siendo reconocida a nivel nacional, brindando un servicio personalizado al cliente.

❖ **Recursos**

Se define como el conjunto de activos tecnológicos de información que dan soporte a los procesos comerciales de la organización como equipos informáticos, equipos de red, sistemas de información, servidores, etc.

1.2.2. Contexto externo

- Entrada: Superintendencia Nacional de Aduanas y de Administración Tributaria, Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, Instituto Nacional de Defensa Civil, Superintendencia de Banca y Seguros del Perú, Banco Central de Reserva del Perú, Revista de activos tecnológicos (ESAN) y lista de oportunidades y amenazas de la empresa 01.
- Técnica utilizada: Lluvia de ideas.
- Herramienta utilizada: Reunión virtual por la plataforma zoom.

LOGO	MATRIZ DE CONTEXTO EXTERNO	Fecha: / /
	Objetivo: Establecer el contexto externo de la organización.	

❖ **Ámbito Legal**

- Legislación fiscal (SUNAT).
- Inspecciones técnicas de seguridad en edificaciones (INDECI).
- Protección al consumidor (INDECOPI).

❖ **Ámbito Económico**

- SBS.
- Economía del país.
- Banco central de reserva del Perú (BCRP).
- Entidades bancarias (BCP, Interbank, Continental, etc).

❖ **Ámbito Competitivo**

- Ferronor SAC.
- Steelmark SA.
- Quiroga SAC.
- 3A Expertos en Acero y Soldadura.

❖ **Ámbito Tecnológico**

Los avances tecnológicos que inciden en nuevos diseños y en la sofisticación de sistemas de información que promueven el uso de la tecnología que facilita la interacción entre grupos de interés, permite crear bases de datos a gran escala, lo cual le brinda a la organización la posibilidad de gestionar un mayor volumen de información y, finalmente, permite automatizar los procesos operacionales.

Fase II: Procesos comerciales

2.1. Identificar los procesos comerciales

- Entrada: Plan estratégico de la empresa 01.

LOGO	MATRIZ DE IDENTIFICACIÓN DE PROCESO COMERCIALES			Fecha: / /
	Objetivo: Identificar los procesos comerciales de la organización.			
Nro.	**CÓDIGO**	**PROCESO**	**DESCRIPCIÓN**	**ÁREA**
1	[P_COM]	Proceso de compras	Consiste en contactar con los proveedores para adquirir un producto que permita disponibilidad stock en almacén.	Administración
2	[P_FAC]	Proceso de facturación	Consiste en concretar la venta a los clientes.	Ventas
3	[P_FPC]	Proceso de Actualización masiva de precios	Consiste en actualizar el precio de venta de los productos, y mantener la lista de precios actualizada.	Administración
4	[P_ALM]	Proceso de almacén	Consiste en recepcionar y almacenar los productos, adquiridos por el área de compras, así como entregar los productos vendidos a los clientes.	Almacén
5	[P_CIC]	Proceso de cierre de caja	Consiste en contabilizar diariamente, la entrada y salida de dinero de una determinada caja.	Ventas
6	[P_COB]	Proceso de cobranzas	Consiste en contactar a los clientes que mantienen deuda, para informar el estado de sus facturas y créditos, ofreciendo opciones de pago.	Ventas
7	[P_TES]	Proceso de tesorería	Consiste en realizar oportunamente los pagos a los proveedores.	Tesorería
8	[P_CON]	Proceso contable	Consiste en brindar información importante de las transacciones comerciales para la obtención de los estados financieros, permitiendo la toma oportuna de decisiones.	Contabilidad

2.2. Análisis de los procesos comerciales

- Entrada: La matriz de identificación de procesos comerciales.

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Identificar las actividades de los procesos comerciales.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
Proceso de Compras	Jefe Administración	Registrar proveedores en el módulo de compras del sistema ERP.	X							X	
		Cotizar precios compra de productos a diferentes proveedores.	X			X		X	X		
		Registra documentos de compra (facturas, notas de crédito, notas de débito) en el módulo de compras del sistema ERP.	X			X				X	
		Aprobación de descuentos de venta en el módulo de facturación del sistema ERP.	X							X	
		Aprobación de cotizaciones generadas por los ejecutivos comerciales en el sistema web de ventas.	X			X					X
		Asignación de ventas de ejecutivos comerciales en el módulo de facturación del sistema ERP.	X							X	
		Cotizar precios de ventas a los clientes en el módulo de facturación del sistema ERP, ya se presencialmente o por correo electrónico.	X			X		X	X	X	
		Consultar reportes (registro de compras, ventas por vendedor, lista de precios) en el sistema ERP.	X			X				X	
Proceso de Facturación	Jefe de ventas	Gestor comercial registra clientes en módulo de facturación del sistema ERP.	X							X	
		Gestor comercial cotiza precios de venta a los clientes en el módulo de facturación del sistema ERP, ya se presencialmente o por correo electrónico.	X			X		X	X	X	
		Gestor comercial registra documentos de venta (facturas, boletas, notas de crédito, notas de débito) en el módulo de facturación del sistema ERP.	X			X				X	

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Identificar las actividades de los procesos comerciales.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
		Gestor comercial contabiliza documentos de ventas (facturas, boletas, notas de crédito, notas de débito) en el módulo de facturación del sistema ERP.	X							X	
		Gestor comercial genera guías de remisión en el módulo de almacén del sistema ERP.	X			X				X	
		Gestor comercial genera guías de transportista en el módulo de almacén del sistema ERP.	X			X				X	
		Ejecutivo comercial externo registra clientes en el sistema web de ventas.		X	X			X			X
		Ejecutivo comercial externo registra hoja de ruta (diariamente) en el sistema web de ventas.		X	X		X	X			X
		Ejecutivo comercial externo cotiza precios de venta en el sistema web de ventas, ya se presencialmente o por correo electrónico.		X	X	X		X	X		X
		Ejecutivo comercial externo registra una venta en el sistema web de ventas.		X	X			X			X
		Consultar reportes (diario de caja, ventas de caja, cuentas por cobrar, lista de precios, ventas por vendedor) en el sistema ERP.		X	X	X				X	X
Proceso de Actualización masiva de precios	Jefe Administración	Actualiza precios de venta en el módulo de actualización masiva de precios del sistema ERP.	X			X				X	
Proceso de almacén	Jefe de Almacen	Generar guías internas en el módulo de almacén del sistema ERP.	X			X				X	
		Crear productos en el módulo de almacén del sistema ERP.	X							X	
		Registrar traslados de productos a otros almacenes de la organización, utilizando el módulo de almacén del sistema ERP.	X			X		X	X	X	
		Consultar reportes (compras de mercadería, stock de productos).	X			X				X	
Proceso de cierre de caja	Jefe de ventas	Registrar el cierre en el módulo de cierre de caja del sistema ERP.	X							X	

LOGO	MATRIZ PARA IDENTIFICAR LAS ACTIVIDADES DE LOS PROCESOS COMERCIALES									Fecha: / /
	Objetivo: Identificar las actividades de los procesos comerciales.									
PROCESO	**RESPONSABLE**	**DESCRIPCION DE LAS ACTIVIDADES**	**ACTIVOS DE TI**								
			COE	**LAP**	**TAB**	**IMP**	**DIA**	**SAI**	**SCE**	**SIE**	**SIV**
Proceso de cobranzas	Jefe de ventas	Registrar línea de crédito en el módulo de cobranzas del sistema ERP.	X							X	
		Cancelar documentos de venta en el módulo de cobranzas del sistema ERP.	X					X	X	X	
		Cancelación de gastos de movilidad en el módulo de cobranzas del sistema ERP.	X					X	X	X	
		Consultar reportes (cuentas por cobrar) en el sistema ERP.	X			X				X	
Proceso de tesorería	Jefe de Tesorería	Registrar proveedores en el módulo de compras del sistema ERP.	X							X	
		Registro de gastos en el módulo de tesorería del sistema ERP.	X							X	
		Cancelar documentos de compra en el módulo de tesorería del sistema ERP.	X					X	X	X	
		Cancelar documentos de gastos en el módulo de tesorería del sistema ERP.	X							X	
		Consultar reportes (cuentas por pagar).	X			X				X	
Proceso contable	Jefe de Contabilidad	Registrar asientos en el módulo contable del sistema ERP.	X							X	
		Aprobación de aperturas de caja en el módulo de cierre de caja del sistema ERP.	X					X	X	X	
		Anulación de documentos de venta (facturas, boletas, notas de crédito, notas de débito) en el módulo de facturación del sistema ERP.	X					X	X	X	
		Anulación de documentos de compra (facturas, notas de crédito, notas de débito) en el módulo de compras del sistema ERP.	X					X	X	X	
		Consulta de reportes (cuentas por cobrar, cuentas por pagar, ventas de caja, registro de compra, estados financieros).	X			X				X	

Fase III: Evaluación del riesgo

3.1. Identificación del riesgo

3.1.1. Identificación de los activos

- Entrada: Lista de activos de TI que intervienen en los procesos comerciales de la empresa 01.

LOGO	MATRIZ DE IDENTIFICACIÓN DE ACTIVOS DE TI				Fecha: / /
	Objetivo: Listar los activos que intervienen en los procesos comerciales.				
Nro.	**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	**ÁREA**	**PROPIETARIO**
1	Proceso	[P_COM]	Proceso de compras	Administración	Jefe Administración
2	Proceso	[P_FAC]	Proceso de facturación	Ventas	Jefe Ventas
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Administración	Jefe Administración
4	Proceso	[P_ALM]	Proceso de almacén	Almacén	Jefe de Almacén
5	Proceso	[P_CIC]	Proceso de cierre de caja	Ventas	Jefe Ventas
6	Proceso	[P_COB]	Proceso de cobranzas	Ventas	Jefe de Ventas
7	Proceso	[P_TES]	Proceso de tesorería	Tesorería	Jefe de Tesorería
8	Proceso	[P_CON]	Proceso contable	Contabilidad	Jefe de Contabilidad
9	Hardware	[HW_COE]	Computadoras de escritorio	TIC's	Jefe de Tic's
10	Hardware	[HW_LAP]	Lapto's	TIC's	Jefe de Tic's
11	Hardware	[HW_TAB]	Tablet's	TIC's	Jefe de Tic's
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	TIC's	Jefe de Tic's
13	Hardware	[HW_SWI]	Switch	TIC's	Jefe de Tic's
14	Hardware	[HW_ACP]	Access Point	TIC's	Jefe de Tic's
15	Hardware	[HW_CAE]	Cableado esrtucturado de red	TIC's	Jefe de Tic's
16	Hardware	[HW_FIR]	Equipo firewall	TIC's	Jefe de Tic's
17	Hardware	[HW_UPS]	UPS	TIC's	Jefe de Tic's
18	Hardware	[HW_IMP]	Impresoras	TIC's	Jefe de Tic's
19	Hardware	[HW_SEA]	Servidor de aplicaciones	TIC's	Jefe de Tic's
20	Hardware	[HW_SED]	Servidor de base datos ERP	TIC's	Jefe de Tic's
21	Software	[SW_BDE]	Base de datos del sistema ERP	TIC's	Jefe de Tic's
22	Software	[SW_SIE]	Sistema ERP	TIC's	Jefe de Tic's
23	Software	[SW_SIV]	Sistema web de ventas	TIC's	Jefe de Tic's
24	Software	[SW_LIS]	Licencias de software	TIC's	Jefe de Tic's

LOGO	MATRIZ DE IDENTIFICACIÓN DE ACTIVOS DE TI				Fecha: / /
	Objetivo: Listar los activos que intervienen en los procesos comerciales.				
Nro.	**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	**ÁREA**	**PROPIETARIO**
25	Software	[SW_PAW]	Página web de la organización	TIC's	Jefe de Tic's
26	Soporte de información	[SIN_BBD]	Backup de base de datos	TIC's	Jefe de Tic's
27	Servicio	[S_SCE]	Servicio de correo electrónico	TIC's	Jefe de Tic's
28	Servicio	[S_SAI]	Servicio de acceso a internet	TIC's	Jefe a Tic's
29	Servicio	[S_WIF]	Servicio de wifi	TIC's	Jefe de Tic's
30	Servicio	[S_PAW]	Servicio de página web	TIC's	Jefe de Tic's

3.1.2. Valoración de los activos

- Entrada: Matriz de identificación de activos de TI.

VALORACIÓN DE CRITERIOS DE LOS ACTIVOS DE TI			
VALOR	**CONFIDENCIALIDAD (C)**	**INTEGRIDAD (I)**	**DISPONIBILIDAD (D)**
5 Muy Alto	Los daños serían catastróficos, la reputación y la imagen de la institución se verían comprometidas.	Tiene que estar correcto y completo al menos en un 99%.	Debe estar disponible al menos el 99% del tiempo.
4 Alto	Los daños serían relevantes, el incidente implicaría a otros procesos.	Tiene que estar correcto y completo al menos en un 75%.	Debe estar disponible al menos el 75% del tiempo.
3 Medio	Daños bajos, el incidente no transcendiera del proceso afectado.	Tiene que estar correcto y completo al menos en un 50%.	Debe estar disponible al menos el 50% del tiempo.
2 Bajo	Daños muy bajos, el incidente no trascendiera del proceso afectado.	No es relevante los errores que tenga o la información que falte.	Debe estar disponible al menos el 10% del tiempo.
1 Muy Bajo	No aplica./ No es relevante para la organización.	No aplica./ No es relevante para la organización.	No aplica./ No es relevante para la organización.

NIVEL DE VALORACIÓN DE LOS ACTIVOS DE TI	
RANGO (resultado de la sumatoria)	**NIVEL DE CRITICIDAD**
De 1 a 3	Muy Bajo
De 4 a 6	Bajo
De 7 a 9	Medio
De 10 a 12	Alto
De 13 a 15	Muy Alto

LOGO	MATRIZ DE VALORACIÓN DE ACTIVOS DE TI						Fecha: / /
	Objetivo: Valorizar los activos de TI, considerando los criterios de confidencialidad, integridad y disponibilidad.						
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**ESCALA DE VALORACIÓN DE CRITERIOS**			**NIVEL DE VALORACIÓN**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**	**C**	**I**	**D**	**TOTAL**	**NIVEL**
1	Proceso	[P_COM]	Proceso de compras	4	5	5	14	Muy Alto
2	Proceso	[P_FAC]	Proceso de facturación	4	5	5	14	Muy Alto
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	5	5	5	15	Muy Alto
4	Proceso	[P_ALM]	Proceso de almacén	4	5	5	14	Muy Alto
5	Proceso	[P_CIC]	Proceso de cierre de caja	3	5	5	13	Muy Alto
6	Proceso	[P_COB]	Proceso de cobranzas	4	5	5	14	Muy Alto
7	Proceso	[P_TES]	Proceso de tesorería	3	5	5	13	Muy Alto
8	Proceso	[P_CON]	Proceso contable	4	5	5	14	Muy Alto
9	Hardware	[HW_COE]	Computadoras de escritorio	3	4	4	11	Alto
10	Hardware	[HW_LAP]	Laptop's	3	4	4	11	Alto
11	Hardware	[HW_TAB]	Tablet's	3	4	4	11	Alto
12	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	2	1	1	4	Bajo
13	Hardware	[HW_SWI]	Switch	4	1	5	10	Alto
14	Hardware	[HW_ACP]	Access Point	4	1	5	10	Alto
15	Hardware	[HW_CAE]	Cableado esrtucturado de red	4	1	5	10	Alto
16	Hardware	[HW_FIR]	Equipo firewall	4	1	5	10	Alto
17	Hardware	[HW_UPS]	UPS	4	2	5	11	Alto
18	Hardware	[HW_IMP]	Impresoras	2	1	2	5	Bajo
19	Hardware	[HW_SEA]	Servidor de aplicaciones	4	4	5	13	Muy Alto
20	Hardware	[HW_SED]	Servidor de base datos ERP	5	5	5	15	Muy Alto
21	Software	[SW_BDE]	Base de datos del sistema ERP	5	5	5	15	Muy Alto
22	Software	[SW_SIE]	Sistema ERP	3	5	5	13	Muy Alto
23	Software	[SW_SIV]	Sistema web de ventas	3	5	5	13	Muy Alto
24	Software	[SW_LIS]	Licencias de software	2	2	4	8	Medio
25	Software	[SW_PAW]	Página web de la organización	5	5	5	15	Muy Alto
26	Soporte de información	[SIN_BBD]	Backup de base de datos	5	5	5	15	Muy Alto
27	Servicio	[S_SCE]	Servicio de correo electrónico	4	2	5	11	Alto
28	Servicio	[S_SAI]	Servicio de acceso a internet	4	1	5	10	Alto
29	Servicio	[S_WIF]	Servicio de wifi	2	1	5	8	Medio
30	Servicio	[S_PAW]	Servicio de página web	5	5	5	15	Muy Alto

3.1.3. Identificar las amenazas

- Entrada: Matriz de identificación de activos de TI.

LOGO	MATRIZ DE IDENTIFICAR AMENAZAS			Fecha: / /
	Objetivo: Determinar las amanezas a las que están expuestos los activos de TI.			
Nro.	IDENTIFICACIÓN DE ACTIVO			AMENAZAS
	CLASIFICACIÓN	CODIGO	ACTIVO	
1	Proceso	[P_COM]	Proceso de compras	Registro de datos errados en el ingreso de una factura de compra
2	Proceso	[P_FAC]	Proceso de facturación	Pérdida de dinero, debido a fallas en el sistema
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Registro de datos errados en la actualización masiva de precios
4	Proceso	[P_ALM]	Proceso de almacén	Pérdida de stock de productos
5	Proceso	[P_CIC]	Proceso de cierre de caja	Cierre no autorizado
6	Proceso	[P_COB]	Proceso de cobranzas	Registro de crédito a clientes sin autorización
7	Proceso	[P_TES]	Proceso de tesorería	Cancelación de facturas erradas a proveedores
8	Proceso	[P_CON]	Proceso contable	Estados financieros incompletos
9	Hardware	[HW_COE]	Computadoras de escritorio	Pérdida de suministro de energía
10	Hardware	[HW_COE]	Computadoras de escritorio	Robo de información
11	Hardware	[HW_LAP]	Laptop's	Pérdida de suministro de energía
12	Hardware	[HW_LAP]	Laptop's	Robo de información
13	Hardware	[HW_TAB]	Tablet's	Pérdida de suministro de energía
14	Hardware	[HW_TAB]	Tablet's	Robo de información
15	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	Deterioro del equipo
16	Hardware	[HW_SWI]	Switch	Pérdida de suministro de energía
17	Hardware	[HW_SWI]	Switch	Deterioro del equipo
18	Hardware	[HW_ACP]	Access Point	Pérdida de suministro de energía
19	Hardware	[HW_ACP]	Access Point	Deterioro del equipo
20	Hardware	[HW_CAE]	Cableado esrtucturado de red	Falla en los equipos de comunicaciones
21	Hardware	[HW_FIR]	Equipo firewall	Deterioro del equipo
22	Hardware	[HW_FIR]	Equipo firewall	Denegación de servicios
23	Hardware	[HW_UPS]	UPS	Falla del equipo

LOGO	MATRIZ DE IDENTIFICAR AMENAZAS			Fecha: / /
	Objetivo: Determinar las amanezas a las que están expuestos los activos de TI.			
Nro.	IDENTIFICACIÓN DE ACTIVO			AMENAZAS
	CLASIFICACIÓN	CODIGO	ACTIVO	
24	Hardware	[HW_IMP]	Impresoras	Deterioro del equipo
25	Hardware	[HW_SEA]	Servidor de aplicaciones	Deterioro del equipo
26	Hardware	[HW_SEA]	Servidor de aplicaciones	Manipulación, robo
27	Hardware	[HW_SEA]	Servidor de aplicaciones	Error de configuración de hardware
28	Hardware	[HW_SED]	Servidor de base datos ERP	Deterioro del equipo
29	Hardware	[HW_SED]	Servidor de base datos ERP	Manipulación, robo
30	Hardware	[HW_SED]	Servidor de base datos ERP	Error de configuración de hardware
31	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado
32	Software	[SW_SIE]	Sistema ERP	Divulgación no autorizada de la información
33	Software	[SW_SIE]	Sistema ERP	Error en el uso del software
34	Software	[SW_SIE]	Sistema ERP	Caída del sistema por sobrecarga de transacciones
35	Software	[SW_SIV]	Sistema web de ventas	Divulgación no autorizada de la información
36	Software	[SW_SIV]	Sistema web de ventas	Error en el uso del software
37	Software	[SW_SIV]	Sistema web de ventas	Caída del sistema por sobrecarga de transacciones
38	Software	[SW_LIS]	Licencias de software	Uso de software ilegal
39	Software	[SW_PAW]	Página web de la organización	Error en el uso del software
40	Soporte de información	[SIN_BBD]	Backup de base de datos	Manipulación de software
41	Servicio	[S_SCE]	Servicio de correo electrónico	Error en el uso del software
42	Servicio	[S_SCE]	Servicio de correo electrónico	Robo de información

LOGO	MATRIZ DE IDENTIFICAR AMENAZAS			Fecha: / /
	Objetivo: Determinar las amanezas a las que están expuestos los activos de TI.			
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**	
43	Servicio	[S_SCE]	Servicio de correo electrónico	Acceso no autorizado
44	Servicio	[S_SAI]	Servicio de acceso a internet	Falla del equipo
45	Servicio	[S_WIF]	Servicio de wifi	Uso no previsto
46	Servicio	[S_PAW]	Servicio de página web	Divulgación no autorizada de la información
47	Servicio	[S_PAW]	Servicio de página web	Error de usuario
48	Servicio	[S_PAW]	Servicio de página web	Acceso no autorizado

3.1.4. Identificar las vulnerabilidades

- Entrada: Matriz de identificar amenazas.

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
1	Proceso	[P_COM]	Proceso de compras	Registro de datos errados en el ingreso de una factura de compra	Falta de validación de datos de entrada
2	Proceso	[P_FAC]	Proceso de facturación	Pérdida de dinero, debido a fallas en el sistema	Carencia de procedimientos para revisar lo facturado
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Registro de datos errados en la actualización masiva de precios	Falta de validación de datos de entrada
4	Proceso	[P_ALM]	Proceso de almacén	Pérdida de stock de productos	Fallas en el software
5	Proceso	[P_CIC]	Proceso de cierre de caja	Cierre no autorizado	Falta de revisiones por parte de caja general

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
6	Proceso	[P_COB]	Proceso de cobranzas	Registro de crédito a clientes sin autorización	Falta de validación de datos de entrada
7	Proceso	[P_TES]	Proceso de tesorería	Cancelación de facturas erradas a proveedores	Falta de reportes de verificación de deudas a proveedores
8	Proceso	[P_CON]	Proceso contable	Estados financieros incompletes	Falta de políticas de cierre de contable
9	Hardware	[HW_COE]	Computadoras de escritorio	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje
10	Hardware	[HW_COE]	Computadoras de escritorio	Robo de información	Falta de backups de información
11	Hardware	[HW_LAP]	Laptop's	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje
12	Hardware	[HW_LAP]	Laptop's	Robo de información	Falta de backups de información
13	Hardware	[HW_TAB]	Tablet's	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje
14	Hardware	[HW_TAB]	Tablet's	Robo de información	Falta de backups de información
15	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
16	Hardware	[HW_SWI]	Switch	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje
17	Hardware	[HW_SWI]	Switch	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
18	Hardware	[HW_ACP]	Access Point	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
19	Hardware	[HW_ACP]	Access Point	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
20	Hardware	[HW_CAE]	Cableado esrtucturado de red	Falla en los equipos de comunicaciones	Cableado desprotegido
21	Hardware	[HW_FIR]	Equipo firewall	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
22	Hardware	[HW_FIR]	Equipo firewall	Denegación de servicios	Carencia de un sistema de información de administración de eventos
23	Hardware	[HW_UPS]	UPS	Falla del equipo	Ausencia de planes de continuidad
24	Hardware	[HW_IMP]	Impresoras	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
25	Hardware	[HW_SEA]	Servidor de aplicaciones	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
26	Hardware	[HW_SEA]	Servidor de aplicaciones	Manipulación, robo	Carencia de políticas de acceso a las instalaciones
27	Hardware	[HW_SEA]	Servidor de aplicaciones	Error de configuración de hardware	Falta de un plan de gestión de cambios
28	Hardware	[HW_SED]	Servidor de base datos ERP	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos
29	Hardware	[HW_SED]	Servidor de base datos ERP	Manipulación, robo	Carencia de políticas de acceso a las instalaciones
30	Hardware	[HW_SED]	Servidor de base datos ERP	Error de configuración de hardware	Falta de un plan de gestión de cambios

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
31	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado	Carencia de una política de asignación de privilegios de acceso
32	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado	Carencia de políticas de contraseñas
33	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado	Modificación no autorizada de BD
34	Software	[SW_SIE]	Sistema ERP	Divulgación no autorizada de la información	Carencia de una política de asignación de privilegios de acceso
35	Software	[SW_SIE]	Sistema ERP	Error en el uso del software	Carencia de manuales de uso de software
36	Software	[SW_SIE]	Sistema ERP	Caída del sistema por sobrecarga de transacciones	Carencia de un sistema de información y procedimientos para administración de eventos
37	Software	[SW_SIV]	Sistema web de ventas	Divulgación no autorizada de la información	Carencia de una política de asignación de privilegios de acceso
38	Software	[SW_SIV]	Sistema web de ventas	Error en el uso del software	Carencia de manuales de uso de software
39	Software	[SW_SIV]	Sistema web de ventas	Caída del sistema por sobrecarga de transacciones	Carencia de un sistema de información para administración de eventos
40	Software	[SW_LIS]	Licencias de software	Uso de software ilegal	Carencia de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual
41	Software	[SW_PAW]	Página web de la organización	Error en el uso del software	Carencia de manuales de uso de software
42	Soporte de información	[SIN_BBD]	Backup de base de datos	Manipulación de software	Falta de copias de respaldo
43	Servicio	[S_SCE]	Servicio de correo electrónico	Error en el uso del software	Carencia de manuales de uso de software

LOGO	MATRIZ DE IDENTIFICAR VULNERABILIDADES				Fecha: / /
	Objetivo: Determinar las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.				
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**
	CLASIFICACIÓN	**CODIGO**	**ACTIVO**		
44	Servicio	[S_SCE]	Servicio de correo electrónico	Robo de información	Falta de backups de información
45	Servicio	[S_SCE]	Servicio de correo electrónico	Acceso no autorizado	Borrado de cuentas por accesos no autorizados por personal que administra el correo
46	Servicio	[S_SAI]	Servicio de acceso a internet	Falla del equipo	Ausencia de planes de continuidad
47	Servicio	[S_WIF]	Servicio de wifi	Uso no previsto	Carencia de políticas de uso del servicio
48	Servicio	[S_PAW]	Servicio de página web	Divulgación no autorizada de la información	Carencia de una política de asignación de privilegios de acceso
49	Servicio	[S_PAW]	Servicio de página web	Error de usuario	Falta de validación de datos de entrada
50	Servicio	[S_PAW]	Servicio de página web	Acceso no autorizado	Ausencia de un sistema de administración de eventos

3.2. Análisis del riesgo

- Entrada: Matriz de identificar vulnerabilidades.

VALORACIÓN DE PROBABILIDAD DE OCURRENCIA		
VALOR	**PROBABILIDAD**	**FRECUENCIA**
5	Casi Cierto	Ocurre diariamente durante un mes.
4	Muy Posible	Ocurre una sola vez durante el mes.
3	Posible	Ocurre una vez al año.
2	Raro	Ocurre una vez cada 5 años.
1	Casi Imposible	No ocurre en un período de 5 años.

VALORACIÓN DE NIVEL DE IMPACTO		
VALOR	**IMPACTO**	**DESCRIPCIÓN**
5	Catastrófico	Se suspenden todas las actividades de los procesos comerciales de la organización.
4	Mayor	Se suspende la atención a los clientes, debido a una caída significativa del sistema, el cual afecta los procesos comerciales de la organización.
3	Moderado	Retrasan la ejecución de los procesos comerciales de la organización.
2	Menor	Limita parcialmente la ejecución de los procesos comerciales de la organización.
1	Insignificante	No afecta la ejecución de los procesos comerciales.

VALORACIÓN DE NIVEL DEL RIESGO		
NIVEL	**RANGO**	**DESCRICPIÓN**
3	12 - 25	Alto
2	5 - 10	Moderado
1	1 - 4	Bajo

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /	
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.									
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**	
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**
1	Proceso	[P_COM]	Proceso de compras	Registro de datos errados en el ingreso de una factura de compra	Falta de validación de datos de entrada	4	4	16	R1	3 Alto
2	Proceso	[P_FAC]	Proceso de facturación	Pérdida de dinero, debido a fallas en el sistema	Carencia de procedimientos para revisar lo facturado	3	3	9	R2	2 Moderado
3	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Registro de datos errados en la actualización masiva de precios	Falta de validación de datos de entrada	4	5	20	R3	3 Alto
4	Proceso	[P_ALM]	Proceso de almacén	Pérdida de stock de productos	Fallas en el software	2	5	10	R4	2 Moderado
5	Proceso	[P_CIC]	Proceso de cierre de caja	Cierre no autorizado	Falta de revisiones por parte de caja general	2	1	2	R5	1 Bajo

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS										Fecha: / /
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
6	Proceso	[P_COB]	Proceso de cobranzas	Registro de crédito a clientes sin autorización	Falta de validación de datos de entrada	4	3	12	R6	3	Alto
7	Proceso	[P_TES]	Proceso de tesorería	Cancelación de facturas erradas a proveedores	Falta de reportes de verificación de deudas a proveedores	1	1	1	R7	1	Bajo
8	Proceso	[P_CON]	Proceso contable	Estados financieros incompletos	Falta de políticas de cierre de contable	1	1	1	R8	1	Bajo
9	Hardware	[HW_COE]	Computadoras de escritorio	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje	3	2	6	R9	2	Moderado
10	Hardware	[HW_COE]	Computadoras de escritorio	Robo de información	Falta de backups de información	4	4	16	R10	3	Alto
11	Hardware	[HW_LAP]	Laptop's	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje	3	2	6	R11	2	Moderado
12	Hardware	[HW_LAP]	Laptop's	Robo de información	Falta de backups de información	4	4	16	R12	3	Alto

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /	
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.									
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**	
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**
13	Hardware	[HW_TAB]	Tablet's	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje	3	2	6	R13	2 Moderado
14	Hardware	[HW_TAB]	Tablet's	Robo de información	Falta de backups de información	4	4	16	R14	3 Alto
15	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	1	1	1	R15	1 Bajo
16	Hardware	[HW_SWI]	Switch	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje	3	3	9	R16	2 Moderado
17	Hardware	[HW_SWI]	Switch	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	3	3	9	R17	2 Moderado
18	Hardware	[HW_ACP]	Access Point	Pérdida de suministro de energía	Susceptibilidad a variaciones en el voltaje	3	3	9	R18	2 Moderado
19	Hardware	[HW_ACP]	Access Point	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	3	2	6	R19	2 Moderado

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /		
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
20	Hardware	[HW_CAE]	Cableado esrtucturado de red	Falla en los equipos de comunicaciones	Cableado desprotegido	4	4	16	R20	3	Alto
21	Hardware	[HW_FIR]	Equipo firewall	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	3	3	9	R21	2	Moderado
22	Hardware	[HW_FIR]	Equipo firewall	Denegación de servicios	Carencia de un sistema de información de administración de eventos	3	2	6	R22	2	Moderado
23	Hardware	[HW_UPS]	UPS	Falla del equipo	Ausencia de planes de continuidad	3	4	12	R23	3	Alto
24	Hardware	[HW_IMP]	Impresoras	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	3	3	9	R24	2	Moderado
25	Hardware	[HW_SEA]	Servidor de aplicaciones	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	4	5	20	R25	3	Alto

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /	
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.									
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**	
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**
26	Hardware	[HW_SEA]	Servidor de aplicaciones	Manipulación, robo	Carencia de políticas de acceso a las instalaciones	4	5	20	R26	3 Alto
27	Hardware	[HW_SEA]	Servidor de aplicaciones	Error de configuración de hardware	Falta de un plan de gestión de cambios	3	4	12	R27	3 Alto
28	Hardware	[HW_SED]	Servidor de base datos ERP	Deterioro del equipo	Ausencia de políticas de mantenimiento preventivo de los equipos	4	5	20	R28	3 Alto
29	Hardware	[HW_SED]	Servidor de base datos ERP	Manipulación, robo	Carencia de políticas de acceso a las instalaciones	4	5	20	R29	3 Alto
30	Hardware	[HW_SED]	Servidor de base datos ERP	Error de configuración de hardware	Falta de un plan de gestión de cambios	3	4	12	R30	3 Alto
31	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado	Carencia de una política de asignación de privilegios de acceso	5	5	25	R31	3 Alto

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /		
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
32	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado	Carencia de políticas de contraseñas	4	4	16	R32	3	Alto
33	Software	[SW_BDE]	Base de datos del sistema ERP	Acceso no autorizado	Modificación no autorizada de BD	4	4	16	R33	3	Alto
34	Software	[SW_SIE]	Sistema ERP	Divulgación no autorizada de la información	Carencia de una política de asignación de privilegios de acceso	4	5	20	R34	3	Alto
35	Software	[SW_SIE]	Sistema ERP	Error en el uso del software	Carencia de manuales de uso de software	4	3	12	R35	3	Alto
36	Software	[SW_SIE]	Sistema ERP	Caída del sistema por sobrecarga de transacciones	Carencia de un sistema de información y procedimientos para administración de eventos	3	3	9	R36	2	Moderado
37	Software	[SW_SIV]	Sistema web de ventas	Divulgación no autorizada de la información	Carencia de una política de asignación de privilegios de acceso	4	5	20	R37	3	Alto

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /	
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.									
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**	
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**
38	Software	[SW_SIV]	Sistema web de ventas	Error en el uso del software	Carencia de manuales de uso de software	4	3	12	R38	3 Alto
39	Software	[SW_SIV]	Sistema web de ventas	Caída del sistema por sobrecarga de transacciones	Carencia de un sistema de información para administración de eventos	3	3	9	R39	2 Moderado
40	Software	[SW_LIS]	Licencias de software	Uso de software ilegal	Carencia de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual	3	3	9	R40	2 Moderado
41	Software	[SW_PAW]	Página web de la organización	Error en el uso del software	Carencia de manuales de uso de software	3	2	6	R41	2 Moderado
42	Soporte de información	[SIN_BBD]	Backup de base de datos	Manipulación de software	Falta de copias de respaldo	4	5	20	R42	3 Alto
43	Servicio	[S_SCE]	Servicio de correo electrónico	Error en el uso del software	Carencia de manuales de uso de software	3	3	9	R43	2 Moderado

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /		
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
44	Servicio	[S_SCE]	Servicio de correo electrónico	Robo de información	Falta de backups de información	2	3	6	R44	2	Moderado
45	Servicio	[S_SCE]	Servicio de correo electrónico	Acceso no autorizado	Borrado de cuentas por accesos no autorizados por personal que administra el correo	3	3	9	R45	2	Moderado
46	Servicio	[S_SAI]	Servicio de acceso a internet	Falla del equipo	Ausencia de planes de continuidad	4	4	16	R46	3	Alto
47	Servicio	[S_WIF]	Servicio de wifi	Uso no previsto	Carencia de políticas de uso del servicio	4	3	12	R47	3	Alto
48	Servicio	[S_PAW]	Servicio de página web	Divulgación no autorizada de la información	Carencia de una política de asignación de privilegios de acceso	2	4	8	R48	2	Moderado
49	Servicio	[S_PAW]	Servicio de página web	Error de usuario	Falta de validación de datos de entrada	3	5	15	R49	3	Alto

LOGO	MATRIZ DE ANÁLISIS DE LOS RIESGOS								Fecha: / /		
	Objetivo: Identificar los valores de probabilidad de ocurrencia e impacto de las vulnerabilidades de las amenazas a las que están expuestos los activos de TI.										
Nro.	**IDENTIFICACIÓN DE ACTIVO**			**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**NIVEL DEL RIESGO**		
	CLASIFICACIÓN	**CÓDIGO**	**ACTIVO**						**CÓDIGO**	**NIVEL**	
50	Servicio	[S_PAW]	Servicio de página web	Acceso no autorizado	Ausencia de un sistema de administración de eventos	2	4	8	R50	2	Moderado

3.3. Valoración del riesgo

- Entrada: Matriz de análisis de los riesgos.
  - **Priorización del riesgo**

IMPACTO	**5 - Catastrófico**		R4	R49	R3 - R25 - R26 - R28 - R29 - R34 - R37 - R42	R31
	4 - Mayor		R48 - R50	R23 - R27 - R30	R1 - R10 - R12 - R14 - R20 - R32 - R33 - R46	
	3 - Moderado		R44	R2 - R16 - R17 - R18 - R21 - R24 - R36 - R39 - R40 - R43 - R45	R6 - R35 - R38 - R47	
	2 - Menor			R9 - R11 - R13 - R19 - R22 - R41		
	1 - Insignificante	R7 - R8 - R15	R5			
		1 - Casi Imposible	**2 - Raro**	**3 - Posible**	**4 - Muy posible**	**5 - Casi Posible**
		PROBABILIDAD				

  - **Nivel de tolerancia**

VALORACIÓN DE TOLERANCIA	
NIVEL DEL RIESGO	**DESCRICPIÓN**
Alto	Intolerable
Moderado	Tolerable
Bajo	Aceptable

LOGO	MATRIZ DE VALORIZACIÓN DEL RIESGO					Fecha: / /
	Objetivo: Indicar la valorización de cada activo de TI.					
NIVEL DEL RIESGO			**IDENTIFICACIÓN DE ACTIVO**			**VALORIZACIÓN**
CÓDIGO	**NIVEL**		**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	
R1	3	Alto	Proceso	[P_COM]	Proceso de compras	Intolerable
R2	2	Moderado	Proceso	[P_FAC]	Proceso de facturación	Tolerable
R3	3	Alto	Proceso	[P_FPC]	Proceso de Actualización masiva de precios	Intolerable
R4	2	Moderado	Proceso	[P_ALM]	Proceso de almacén	Tolerable
R5	1	Bajo	Proceso	[P_CIC]	Proceso de cierre de caja	Aceptable
R6	3	Alto	Proceso	[P_COB]	Proceso de cobranzas	Intolerable
R7	1	Bajo	Proceso	[P_TES]	Proceso de tesorería	Aceptable
R8	1	Bajo	Proceso	[P_CON]	Proceso contable	Aceptable
R9	2	Moderado	Hardware	[HW_COE]	Computadoras de escritorio	Tolerable
R10	3	Alto	Hardware	[HW_COE]	Computadoras de escritorio	Intolerable
R11	2	Moderado	Hardware	[HW_LAP]	Laptop's	Tolerable
R12	3	Alto	Hardware	[HW_LAP]	Laptop's	Intolerable
R13	2	Moderado	Hardware	[HW_TAB]	Tablet's	Tolerable
R14	3	Alto	Hardware	[HW_TAB]	Tablet's	Intolerable
R15	1	Bajo	Hardware	[HW_DIA]	Dispositivos de almacenamiento USB	Aceptable
R16	2	Moderado	Hardware	[HW_SWI]	Switch	Tolerable
R17	2	Moderado	Hardware	[HW_SWI]	Switch	Tolerable
R18	2	Moderado	Hardware	[HW_ACP]	Access Point	Tolerable
R19	2	Moderado	Hardware	[HW_ACP]	Access Point	Tolerable
R20	3	Alto	Hardware	[HW_CAE]	Cableado esrtucturado de red	Intolerable
R21	2	Moderado	Hardware	[HW_FIR]	Equipo firewall	Tolerable

LOGO	MATRIZ DE VALORIZACIÓN DEL RIESGO					Fecha: / /
	Objetivo: Indicar la valorización de cada activo de TI.					
NIVEL DEL RIESGO			**IDENTIFICACIÓN DE ACTIVO**			**VALORIZACIÓN**
CÓDIGO	**NIVEL**		**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	
R22	2	Moderado	Hardware	[HW_FIR]	Equipo firewall	Tolerable
R23	3	Alto	Hardware	[HW_UPS]	UPS	Intolerable
R24	2	Moderado	Hardware	[HW_IMP]	Impresoras	Tolerable
R25	3	Alto	Hardware	[HW_SEA]	Servidor de aplicaciones	Intolerable
R26	3	Alto	Hardware	[HW_SEA]	Servidor de aplicaciones	Intolerable
R27	3	Alto	Hardware	[HW_SEA]	Servidor de aplicaciones	Intolerable
R28	3	Alto	Hardware	[HW_SED]	Servidor de base datos ERP	Intolerable
R29	3	Alto	Hardware	[HW_SED]	Servidor de base datos ERP	Intolerable
R30	3	Alto	Hardware	[HW_SED]	Servidor de base datos ERP	Intolerable
R31	3	Alto	Software	[SW_BDE]	Base de datos del sistema ERP	Intolerable
R32	3	Alto	Software	[SW_BDE]	Base de datos del sistema ERP	Intolerable
R33	3	Alto	Software	[SW_BDE]	Base de datos del sistema ERP	Intolerable
R34	3	Alto	Software	[SW_SIE]	Sistema ERP	Intolerable
R35	3	Alto	Software	[SW_SIE]	Sistema ERP	Intolerable
R36	2	Moderado	Software	[SW_SIE]	Sistema ERP	Tolerable
R37	3	Alto	Software	[SW_SIV]	Sistema web de ventas	Intolerable
R38	3	Alto	Software	[SW_SIV]	Sistema web de ventas	Intolerable

LOGO	MATRIZ DE VALORIZACIÓN DEL RIESGO					Fecha: / /
	Objetivo: Indicar la valorización de cada activo de TI.					
NIVEL DEL RIESGO			**IDENTIFICACIÓN DE ACTIVO**			**VALORIZACIÓN**
CÓDIGO	**NIVEL**		**CLASIFICACIÓN**	**CÓDIGO**	**ACTIVO**	
R39	2	Moderado	Software	[SW_SIV]	Sistema web de ventas	Tolerable
R40	2	Moderado	Software	[SW_LIS]	Licencias de software	Tolerable
R41	2	Moderado	Software	[SW_PAW]	Página web de la organización	Tolerable
R42	3	Alto	Soporte de información	[SIN_BBD]	Backup de base de datos	Intolerable
R43	2	Moderado	Servicio	[S_SCE]	Servicio de correo electrónico	Tolerable
R44	2	Moderado	Servicio	[S_SCE]	Servicio de correo electrónico	Tolerable
R45	2	Moderado	Servicio	[S_SCE]	Servicio de correo electrónico	Tolerable
R46	3	Alto	Servicio	[S_SAI]	Servicio de acceso a internet	Intolerable
R47	3	Alto	Servicio	[S_WIF]	Servicio de wifi	Intolerable
R48	2	Moderado	Servicio	[S_PAW]	Servicio de página web	Tolerable
R49	3	Alto	Servicio	[S_PAW]	Servicio de página web	Intolerable
R50	2	Moderado	Servicio	[S_PAW]	Servicio de página web	Tolerable

Fase IV: Tratamiento del riesgo

4.1. Selección de opciones de tratamiento de riesgo

- Entrada: Matriz de valoración del riesgo.

OPCIONES DE TRATAMIENTO	
ESTRATEGIA	**DESCRIPCIÓN**
Evitar	Dejar de realizar las actividades o las condiciones que generen el riesgo.
Transferir-Compartir	Reducir la frecuencia y el impacto al transferir o compartir el riesgo. Suele darse a través de la contratación de seguro, la externalización de servicios o instrumentos de mercado de capital a largo plazo. La organización sigue siendo propietaria del riesgo.
Mitigar	Ejecutar acciones para reducir la frecuencia e impacto de un riesgo. Implementar procesos de gestión de riesgos para introducir, eliminar, modificar controles que permitan que el riesgo residual puede ser reevaluado como aceptable.
Aceptar	Se cuenta con información de sustento acerca del riesgo y se reconoce la exposición a la pérdida; sin embargo, no se toman acciones relativas a un riesgo en particular. La organización acepta la pérdida en caso ocurra.

4.2. Proponer planes de tratamiento de riesgo

- Entrada: Matriz de valoración del riesgo.

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE001
Nombre:	Implementar un plan de contingencia para restablecer los servicios de TI, sin afectar la continuidad de los procesos comerciales.
Estrategia:	◯ Aceptar ◯ Mitigar ● Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_UPS] UPS. * [S_SAI] Servicio de acceso a internet.	
Riesgos a Tratar	
R23, R46.	
Objetivo	
Restablecer los servicios que afecten los procesos comerciales de la organización en el menor tiempo de posible.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	

Recursos
* Jefe de Tic's. * Analista de Tic's.
Duración
30 días hábiles, considerando 8 horas diarias.
Presupuesto
S/. 1,500.00.

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE002
Nombre:	Implementar una política de mantenimiento preventivo a equipos informáticos.
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_SEA] Servidor de aplicaciones. * [HW_SED] Servidor de base datos ERP.	
Riesgos a Tratar	
R25, R28.	
Objetivo	
Mitigar el riesgo de fallas que interrumpan la continuidad operativa y alargar el tiempo de vida útil de los equipos informáticos.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
30 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 1,500.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE003
Nombre:	Implementar un plan de mantenimiento del cableado estructurado de red para garantizar un rendimiento óptimo de la red.
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_CAE] Cableado estructurado de red.	
Riesgos a Tratar	
R20.	
Objetivo	
Mitigar el riesgo de transmitir datos de forma más rápida y confidencial, optimizando los recursos de los que se dispone.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
45 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 6,000.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE004
Nombre:	Implementar una política para el uso e instalación del software, mediante un documento de comunicación técnica que brinde asistencia a los usuarios de la organización.
Estrategia:	◯ Aceptar ◯ Mitigar ● Evitar ◯ Transferir - Compartir
Dato de Activo	
* [SW_SIE] Sistema ERP. * [SW_SIV] Sistema web de ventas.	
Riesgos a Tratar	
R35, R38.	
Objetivo	
Definir pautas para el uso del software en la organización, incentivando su mejor aprovechamiento, y el aseguramiento de la integridad de la información.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
40 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 2,500.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE005
Nombre:	Implementar una política de control de acceso físico a las instalaciones del DataCenter, para proteger la infraestructura tecnológica en la organización.
Estrategia:	◯ Aceptar ◉ Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_SEA] Servidor de aplicaciones. * [HW_SED] Servidor de base datos ERP.	
Riesgos a Tratar	
R26, R29	
Objetivo	
Establecer los lineamientos generales para controlar el acceso físico a las instalaciones del DataCenter, reduciendo los riesgos de acceso no autorizado para prevenir la pérdida de información, daños a los recursos físicos, entre otros.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
40 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 2,500.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE006
Nombre:	Implementar una política de gestión de contraseñas y buenas prácticas para favorecer el acceso y el uso autorizado a los datos y servicios de la organización.
Estrategia:	◯ Aceptar ◉ Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_CAE] Base de datos del sistema ERP.	
Riesgos a Tratar	
R32.	
Objetivo	
Garantizar que las credenciales de autenticación se generen, actualicen y revoquen de forma óptima y segura, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
30 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 2,000.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE007
Nombre:	Implementar una política de uso y seguridad de la red inalámbrica de la organización.
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [S_WIF] Servicio de wifi.	
Riesgos a Tratar	
R47.	
Objetivo	
Asegurar que todos los usuarios de la red inalámbrica reciban un nivel de servicio de calidad en cuanto a confiabilidad, integridad, disponibilidad de servicio y seguridad.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
30 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 2,000.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE008
Nombre:	Implementar una política de control de acceso de datos, para administrar y controlar el acceso a los sistemas de información y base de datos.
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_CAE] Base de datos del sistema ERP. * [SW_SIE] Sistema ERP. * [SW_SIV] Sistema web de ventas.	
Riesgos a Tratar	
R31, R33, R34, R37.	
Objetivo	
Establecer los niveles de acceso apropiados a la información de la organización, brindando y asegurando la confidencialidad, integridad y disponibilidad de los datos, los cuales serán autorizados por la jefatura correspondiente.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
40 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 2,500.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE009
Nombre:	Implementar un plan para el respaldo de la información, que permita obtener la disponibilidad de los datos de los equipos informáticos, ante un evento.
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_COE] Computadoras de escritorio. * [HW_LAP] Laptop's. * [HW_TAB] Tablet's.	
Riesgos a Tratar	
R10, R12, R14.	
Objetivo	
Restaurar de forma eficiente la copia de seguridad, asegurando la continuidad de los procesos comerciales de la organización.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
20 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 1,200.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE010
Nombre:	Implementar un plan para asegurar el respaldo, custodia y restauración oportuna de la información, para evitar impactos que afecten en forma negativa a la organización.
Estrategia:	◯ Aceptar ◯ Mitigar ● Evitar ◯ Transferir - Compartir
Dato de Activo	
* [SIN_BBD] Backup de base de datos.	
Riesgos a Tratar	
R42	
Objetivo	
Disminuir el riesgo de impacto en la reanudación de las actividades de los procesos comerciales de la organización.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
30 días hábiles, considerando 8 horas diarias.	
Presupuesto	
S/. 2,000.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE011
Nombre:	Implementar un procedimiento de gestión de cambios, basado en los principios de las mejores prácticas de ITIL.
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [HW_SEA] Servidor de aplicaciones. * [HW_SED] Servidor de base datos ERP.	
Riesgos a Tratar	
R27, R30.	
Objetivo	
Minimizar el impacto de las incidencias que se presenten en la organización, por los cambios que se realicen para garantizar eficientemente la calidad del servicio.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
Experto en ITIL.	
Duración	
45 días hábiles, considerando 8 horas diarios.	
Presupuesto	
S/. 5,500.00.	

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO	
Código:	PE012
Nombre:	Implementar controles de validación de datos de entrada en el módulo de ventas, compras y cobranzas, basándose en estándares de calidad de desarrollo de software.
Estrategia:	◯ Aceptar ◉ Mitigar ◯ Evitar ◯ Transferir - Compartir
Dato de Activo	
* [S_PAW] Servicio de página web. * [P_COM] Proceso de compras. * [P_FPC] Proceso de Actualización masiva de precios. * [P_COB] Proceso de cobranzas.	
Riesgos a Tratar	
R1, R3, R6, R49.	
Objetivo	
Minimizar el riesgo de errores de ingresó de datos en el módulo de ventas, compras y cobranzas para garantizar la fiabilidad de los datos.	
Área Responsable	
Jefatura de Tecnologías de la Información y Comunicaciones.	
Recursos	
* Jefe de Tic's. * Analista de Tic's.	
Duración	
35 días hábiles, considerando 8 horas diarios.	
Presupuesto	
S/. 4,000.00.	

Fase V: Seguimineto y revisión

5.1. Seguimiento y revisión

- Entrada: Matriz de plan de tratamiento de riesgo.

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE001		
Nombre:	Implementar un plan de contingencia para restablecer los servicios de TI, sin afectar la continuidad de los procesos comerciales.		
Estrategia:	◯ Aceptar ◯ Mitigar ● Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_UPS] UPS. * [S_SAI] Servicio de acceso a internet.			
Riesgos a Tratar			
R23, R46.			
Objetivo			
Restablecer los servicios que afecten los procesos comerciales de la organización en el menor tiempo de posible.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
30 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 1,500.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	60%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	-Garantizar la disponibilidad del servicio de internet 24/7. -Garantizar el correcto funcionamiento del UPS, realizando mantenimientos continuos al equipo.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE002		
Nombre:	Implementar una política de mantenimiento preventivo a equipos informáticos.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_SEA] Servidor de aplicaciones. * [HW_SED] Servidor de base datos ERP.			
Riesgos a Tratar			
R25, R28.			
Objetivo			
Mitigar el riesgo de fallas que interrumpan la continuidad operativa y alargar el tiempo de vida útil de los equipos informáticos.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
30 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 1,500.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	50%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Garantizar el funcionamiento óptimo de los equipos en un 100%.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE003		
Nombre:	Implementar un plan de mantenimiento del cableado estructurado de red para garantizar un rendimiento óptimo de la red.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_CAE] Cableado estructurado de red.			
Riesgos a Tratar			
R20.			
Objetivo			
Mitigar el riesgo de transmitir datos de forma más rápida y confidencial, optimizando los recursos de los que se dispone.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
45 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 6,000.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	60%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Mejorar la calidad del servicio de red en un 80%.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE004		
Nombre:	Implementar una política para el uso e instalación del software, mediante un documento de comunicación técnica que brinde asistencia a los usuarios de la organización.		
Estrategia:	◯ Aceptar ◯ Mitigar ● Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [SW_SIE] Sistema ERP. * [SW_SIV] Sistema web de ventas.			
Riesgos a Tratar			
R35, R38.			
Objetivo			
Definir pautas para el uso del software en la organización, incentivando su mejor aprovechamiento, y el aseguramiento de la integridad de la información.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
40 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 2,500.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	60%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Aprobación de los manuales de software por parte de la gerencia de administración y finanzas. - Aplicación del manual por parte del área de TIC's.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE005		
Nombre:	Implementar una política de control de acceso físico a las instalaciones del DataCenter, para proteger la infraestructura tecnológica en la organización.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_SEA] Servidor de aplicaciones. * [HW_SED] Servidor de base datos ERP.			
Riesgos a Tratar			
R26, R29.			
Objetivo			
Establecer los lineamientos generales para controlar el acceso físico a las instalaciones del DataCenter, reduciendo los riesgos de acceso no autorizado para prevenir la pérdida de información, daños a los recursos físicos, entre otros.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
40 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 2,500.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	50%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Controlar los accesos al DataCenter mediante un sistema de biométrico. - Monitorear con un sistema de videogilancia la infraestructura del DataCenter.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE006		
Nombre:	Implementar una política de gestión de contraseñas y buenas prácticas para favorecer el acceso y el uso autorizado a los datos y servicios de la organización.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_CAE] Base de datos del sistema ERP.			
Riesgos a Tratar			
R32.			
Objetivo			
Garantizar que las credenciales de autenticación se generen, actualicen y revoquen de forma óptima y segura, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
30 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 2,000.00			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	50%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Reducir el número de accesos no autorizados por ausencia de una política de gestión de contraseñas.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE007		
Nombre:	Implementar una política de uso y seguridad de la red inalámbrica de la organización.		
Estrategia:	◯ Aceptar ◉ Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [S_WIF] Servicio de wifi.			
Riesgos a Tratar			
R47.			
Objetivo			
Asegurar que todos los usuarios de la red inalámbrica reciban un nivel de servicio de calidad en cuanto a confiabilidad, integridad, disponibilidad de servicio y seguridad.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
30 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 2,000.00			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	50%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Controlar los accesos de los usuarios a la red inalámbrica. - Monitorear el rendimiento y la calidad del servicio de la red inalámbrica.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE008		
Nombre:	Implementar una política de control de acceso de datos, para administrar y controlar el acceso a los sistemas de información y base de datos.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_CAE] Base de datos del sistema ERP. * [SW_SIE] Sistema ERP. * [SW_SIV] Sistema web de ventas.			
Riesgos a Tratar			
R31, R33, R34, R37.			
Objetivo			
Establecer los niveles de acceso apropiados a la información de la organización, brindando y asegurando la confidencialidad, integridad y disponibilidad de los datos, los cuales serán autorizados por la jefatura correspondiente.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
40 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 2,500.00			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	60%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Impedir el acceso no autorizado a los sistemas de información y base de datos - Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización. - Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas de información.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE009		
Nombre:	Implementar un plan para el respaldo de la información, que permita obtener la disponibilidad de los datos de los equipos informáticos, ante un evento.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_COE] Computadoras de escritorio. * [HW_LAP] Laptop's. * [HW_TAB] Tablet's.			
Riesgos a Tratar			
R10, R12, R14.			
Objetivo			
Restaurar de forma eficiente la copia de seguridad, asegurando la continuidad de los procesos comerciales de la organización.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
20 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 1,200.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	80%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Gestionar tareas programadas de copias de respaldo de información.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE010		
Nombre:	Implementar un plan para asegurar el respaldo, custodia y restauración oportuna de la información, para evitar impactos que afecten en forma negativa a la organización.		
Estrategia:	◯ Aceptar ◯ Mitigar ● Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [SIN_BBD] Backup de base de datos.			
Riesgos a Tratar			
R42.			
Objetivo			
Disminuir el riesgo de impacto en la reanudación de las actividades de los procesos comerciales de la organización.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
30 días hábiles, considerando 8 horas diarias.			
Presupuesto			
S/. 2,000.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	60%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Minimizar el riesgo de pérdida de información.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE011		
Nombre:	Implementar un procedimiento de gestión de cambios, basado en los principios de las mejores prácticas de ITIL.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [HW_SEA] Servidor de aplicaciones. * [HW_SED] Servidor de base datos ERP.			
Riesgos a Tratar			
R27, R30.			
Objetivo			
Minimizar el impacto de las incidencias que se presenten en la organización, por los cambios que se realicen para garantizar eficientemente la calidad del servicio.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
Experto en ITIL.			
Duración			
45 días hábiles, considerando 8 horas diarios.			
Presupuesto			
S/. 5,500.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	50%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Aplicar los procedimientos diseños para la gestión de cambios en el área de TIC's.		

MATRIZ DE SEGUIMIENTO Y REVISIÓN DE PLAN			
Código:	PE012		
Nombre:	Implementar controles de validación de datos de entrada en el módulo de ventas, compras y cobranzas, basándose en estándares de calidad de desarrollo de software.		
Estrategia:	◯ Aceptar ● Mitigar ◯ Evitar ◯ Transferir - Compartir		
Dato de Activo			
* [S_PAW] Servicio de página web. * [P_COM] Proceso de compras. * [P_FPC] Proceso de Actualización masiva de precios. * [P_COB] Proceso de cobranzas.			
Riesgos a Tratar			
R1, R3, R6, R49.			
Objetivo			
Minimizar el riesgo de errores de ingresó de datos en el módulo de ventas, compras y cobranzas para garantizar la fiabilidad de los datos.			
Área Responsable			
Jefatura de Tecnologías de la Información y Comunicaciones.			
Recursos			
* Jefe de Tic's. * Analista de Tic's.			
Duración			
35 días hábiles, considerando 8 horas diarios.			
Presupuesto			
S/. 4,000.00.			
SEGUIMIENTO Y REVISIÓN			
Responsable:	- Gerencia de Administración y Finanzas. - Gerencia Comercial.		
Porcentaje de Cumpliento:	60%.	**Estado:**	En ejecución.
Resultados Esperados del Plan:	- Garantizar el procesamiento adecuado de los datos ingresados por el usuario en los sistemas de información.		

Anexo 9: Informe de Opinión de Experto

INFORME DE OPINIÓN DE EXPERTO

MODELO DE GESTIÓN DE RIESGOS DE TI PARA DAR SOPORTE A LOS PROCESOS COMERCIALES DE LAS EMPRESAS DISTRIBUIDORAS DE MATERIALES DE CONSTRUCCIÓN EN LA REGIÓN LAMBAYEQUE

Objetivo:

El objetivo del presente informe es someter a evaluación el modelo propuesto de gestión de riesgos, el cual surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, ISO 27005, COBIT 5, MAGERIT Y OCTAVE), para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción en la región Lambayeque.

DATOS GENERALES DEL EXPERTO	
Apellidos y Nombres:	
Grado Académico:	
Área de Experiencia Profesional:	
Tiempo de experiencia:	

ESCALA DE CALIFICACIÓN
1: Total desacuerdo. 2: En desacuerdo. 3: Ni de acuerdo ni en desacuerdo. 4: De acuerdo. 5: Totalmente de acuerdo.

INSTRUCCIONES
Señale con "X" la opción elegida.

FASE	**ACTIVIDAD**		**ESCALA DE LIKERT**					**OBERVACIÓN**
			1	**2**	**3**	**4**	**5**	
FASE I: ALCANCE Y CONTEXTO	DEFINIR EL ALCANCE							
	ESTABLECER EL CONTEXTO	CONTEXTO INTERNO						
		CONTEXTO EXTERNO						

FASE II: PROCESOS COMERCIALES	IDENTIFICAR LOS PROCESOS COMERCIALES							
	ANALISIS DE LOS PROCESOS COMERCIALES							
FASE III: EVALUACION DEL RIESGO	IDENTIFICACION DEL RIESGO	IDENTIFICACION DE LOS ACTIVOS						
		VALORACION DE LOS ACTIVOS						
		INDENTIFICAR LAS AMENAZAS						
		IDENTIFICAR LAS VULNERABILIDADES						
	ANALISIS DEL RIESGO							
	VALORACION DEL RIESGO							
FASE IV: TRATAMIENTO DEL RIESGO	SELECCION DE OPCIONES DE TRATAMIENTO DE RIESGO							
	PROPONER PLANES DE TRATAMIENTO DE RIESGO							
FASE V: SEGUIMIENTO Y REVISION	SEGUIMIENTO Y REVISION							

DESFAVORABLE	
DEBE MEJORAR	
ACEPTACIÓN	

FIRMA DEL EXPERTO

Anexo 10: Informe de Validación de Expertos

INFORME DE OPINIÓN DE EXPERTO

MODELO DE GESTIÓN DE RIESGOS DE TI PARA DAR SOPORTE A LOS PROCESOS COMERCIALES DE LAS EMPRESAS DISTRIBUIDORAS DE MATERIALES DE CONSTRUCCIÓN EN LA REGIÓN LAMBAYEQUE

Objetivo:

El objetivo del presente informe es someter a evaluación el modelo propuesto de gestión de riesgos, el cual surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, ISO 27005, COBIT 5, MAGERIT Y OCTAVE), para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción en la región Lambayeque.

DATOS GENERALES DEL EXPERTO	
Apellidos y Nombres:	GILBERTO CARRIÓN BARCO
Grado Académico:	DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS
Area de Experiencia Profesional:	INFRAESTRUCTURA TECNOLÓGICA
Tiempo de experiencia:	16 años

ESCALA DE CALIFICACIÓN
1: Total desacuerdo. 2: En desacuerdo. 3: Ni de acuerdo ni en desacuerdo. 4: De acuerdo. 5: Totalmente de acuerdo.

INSTRUCCIONES
Señale con "X" la opción elegida.

FASE	**ACTIVIDAD**		**ESCALA DE LIKERT**					**OBSERVACIÓN**
			1	**2**	**3**	**4**	**5**	
FASE I: ALCANCE Y CONTEXTO	DEFINIR EL ALCANCE						X	
	ESTABLECER EL CONTEXTO	CONTEXTO INTERNO					X	
		CONTEXTO EXTERNO					X	

FASE II: PROCESOS COMERCIALES	IDENTIFICAR LOS PROCESOS COMERCIALES						X	
	ANÁLISIS DE LOS PROCESOS COMERCIALES						X	
FASE III: EVALUACIÓN DEL RIESGO	IDENTIFICACIÓN DEL RIESGO	IDENTIFICACIÓN DE LOS ACTIVOS					X	
		VALORACIÓN DE LOS ACTIVOS					X	
		IDENTIFICAR LAS AMENAZAS					X	
		IDENTIFICAR LAS VULNERABILIDADES					X	
	ANÁLISIS DEL RIESGO						X	
	VALORACIÓN DEL RIESGO						X	
FASE IV: TRATAMIENTO DEL RIESGO	SELECCIÓN DE OPCIONES DE TRATAMIENTO DE RIESGO						X	
	PROPONER PLANES DE TRATAMIENTO DE RIESGO						X	
FASE V: SEGUIMIENTO Y REVISIÓN	SEGUIMIENTO Y REVISIÓN						X	

DESFAVORABLE	
DEBE MEJORAR	
ACEPTACIÓN	X

COMENTARIO:

El modelo propuesto contiene las fases y actividades suficientes y necesarias para ser consideradas validas; por lo tanto, aptas para ser aplicadas en el logro de los objetivos que se plantean en la investigación

Dr. Gilberto Carrión Barco
DNI: 16720146

INFORME DE OPINIÓN DE EXPERTO

MODELO DE GESTIÓN DE RIESGOS DE TI PARA DAR SOPORTE A LOS PROCESOS COMERCIALES DE LAS EMPRESAS DISTRIBUIDORAS DE MATERIALES DE CONSTRUCCIÓN EN LA REGIÓN LAMBAYEQUE

Objetivo:

El objetivo del presente informe es someter a evaluación el modelo propuesto de gestión de riesgos, el cual surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, ISO 27005, COBIT 5, MAGERIT Y OCTAVE), para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción en la región Lambayeque.

DATOS GENERALES DEL EXPERTO	
Apellidos y Nombres:	MINO PÉREZ KARINA ARACELI
Grado Académico:	MAESTRO EN INGENIERIA DE SISTEMAS CON MECION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE
Area de Experiencia Profesional:	TECNOLOGIAS DE LA INFORMACIÓN
Tiempo de experiencia:	12 AÑOS

ESCALA DE CALIFICACIÓN

1: Total desacuerdo.
2: En desacuerdo.
3: Ni de acuerdo ni en desacuerdo.
4: De acuerdo.
5: Totalmente de acuerdo.

INSTRUCCIONES

Señale con "X" la opción elegida.

FASE	**ACTIVIDAD**		**ESCALA DE LIKERT**					**OBERVACIÓN**
			1	**2**	**3**	**4**	**5**	
FASE I: ALCANCE Y CONTEXTO	DEFINIR EL ALCANCE						**X**	
	ESTABLECER EL CONTEXTO	CONTEXTO INTERNO					**X**	
		CONTEXTO EXTERNO				**X**		

FASE II: PROCESOS COMERCIALES	IDENTIFICAR LOS PROCESOS COMERCIALES					X		
	ANALISIS DE LOS PROCESOS COMERCIALES						X	
FASE III: EVALUACION DEL RIESGO	IDENTIFICACION DEL RIESGO	IDENTIFICACION DE LOS ACTIVOS					X	
		VALORACION DE LOS ACTIVOS				X		
		INDENTIFICAR LAS AMENAZAS					X	
		IDENTIFICAR LAS VULNERABILIDADES					X	
	ANALISIS DEL RIESGO						X	
	VALORACION DEL RIESGO						X	
FASE IV: TRATAMIENTO DEL RIESGO	SELECCION DE OPCIONES DE TRATAMIENTO DE RIESGO					X		
	PROPONER PLANES DE TRATAMIENTO DE RIESGO					X		
FASE V: SEGUIMIENTO Y REVISION	SEGUIMIENTO Y REVISION					X		

DESFAVORABLE	
DEBE MEJORAR	
ACEPTACION	X

***COMENTARIO**: El presente modelo, cumple con los requerimientos exigidos para el análisis y valoración de riesgos tecnológicos, que permitirán al analista, aplicar el tratamiento adecuado para la atenuación del riesgo, en los procesos comerciales de las empresas distribuidoras de materiales de construcción de la región Lambayeque.*

Mg. Karina Araceli Mino Pérez

DNI 17633083

INFORME DE OPINIÓN DE EXPERTO

MODELO DE GESTIÓN DE RIESGOS DE TI PARA DAR SOPORTE A LOS PROCESOS COMERCIALES DE LAS EMPRESAS DISTRIBUIDORAS DE MATERIALES DE CONSTRUCCIÓN EN LA REGIÓN LAMBAYEQUE

Objetivo:

El objetivo del presente informe es someter a evaluación el modelo propuesto de gestión de riesgos, el cual surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, ISO 27005, COBIT 5, MAGERIT Y OCTAVE), para dar soporte a los procesos comerciales de las empresas distribuidoras de materiales de construcción en la región Lambayeque.

DATOS GENERALES DEL EXPERTO	
Apellidos y Nombres:	PUICAN GUTIERREZ, ROBERT EDGAR
Grado Académico:	MAGISTER EN ADMINISTRACIÓN, CON MENCION EN GERENCIA EMPRESARIAL
Área de Experiencia Profesional:	REDES DE COMPUTADORES, BASE DE DATOS, SEGURIDAD INFORMATICA, AUDITORIA DE SISTEMAS
Tiempo de experiencia:	20 AÑOS

ESCALA DE CALIFICACION

1: Total desacuerdo.
2: En desacuerdo.
3: Ni de acuerdo ni en desacuerdo.
4: De acuerdo.
5: Totalmente de acuerdo.

INSTRUCCIONES

Señale con "X" la opción elegida.

FASE	ACTIVIDAD		ESCALA DE LIKERT					OBERVACIÓN
			1	2	3	4	5	
FASE I: ALCANCE Y CONTEXTO	DEFINIR EL ALCANCE					X		
	ESTABLECER EL CONTEXTO	CONTEXTO INTERNO				X		
		CONTEXTO EXTERNO					X	
	IDENTIFICAR LOS PROCESOS COMERCIALES						X	

FASE II: PROCESOS COMERCIALES	ANALISIS DE LOS PROCESOS COMERCIALES					X		
FASE III: EVALUACION DEL RIESGO	IDENTIFICACION DEL RIESGO	IDENTIFICACION DE LOS ACTIVOS				X		
		VALORACION DE LOS ACTIVOS				X		
		INDENTIFICAR LAS AMENAZAS				X		
		IDENTIFICAR LAS VULNERABILIDADES				X		
	ANALISIS DEL RIESGO					X		
	VALORACION DEL RIESGO					X		
FASE IV: TRATAMIENTO DEL RIESGO	SELECCION DE OPCIONES DE TRATAMIENTO DE RIESGO						X	
	PROPONER PLANES DE TRATAMIENTO DE RIESGO						X	
FASE V: SEGUIMIENTO Y REVISION	SEGUIMIENTO Y REVISION						X	

DESFAVORABLE	
DEBE MEJORAR	
ACEPTACION	X

MG. ROBERT EDGAR PUICAN GUTIERREZ

DNI 16769559

Anexo 11: Cuestionario para medir el nivel de utilidad del modelo propuesto en la empresa 01

CUESTIONARIO PARA MEDIR EL NIVEL DE UTILIDAD DEL MODELO PROPUESTO EN LA EMPRESA 01

Dirigida: Jefe de TI.

Fecha : _____

Nombre : _____

Procedimiento: El siguiente cuestionario tiene por finalidad conocer la utilidad del modelo propuesto de gestión de riesgos de TI para dar soporte a los procesos comerciales en la empresa donde labora.

Indicaciones: Marque con una X la respuesta seleccionada por usted. Revisar la guía para el desarrollo del cuestionario

N°	PREGUNTA	SI	NO	COMENTARIO
1	¿A partir del modelo propuesto se puede definir el alcance de la gestión de riesgos?			
2	¿El modelo propuesto permite a la organización establecer el contexto externo e interno en el cual opera la organización?			
3	¿A partir del modelo propuestos se puede identificar los procesos o actividades que apoyan la estrategia comercial de la organización?			
4	¿En el modelo propuesto se logra identificar los activos de TI que intervienen en los procesos comerciales de la organización?			
5	¿El modelo propuesto permite a la organización clasificar los de activos de TI?			
6	¿La valoración de criterios de los activos de TI como confidencialidad, integridad y disponibilidad en el modelo propuesto, se ajusta a la realidad de la organización?			
7	¿En el modelo propuesto se identifican las amenazas y vulnerabilidades a las que están expuestos los activos de TI?			
8	¿En el modelo propuesto se puede identificar, clasificar y analizar los diferentes escenarios de riesgos de TI, en la organización?			
9	¿En el modelo propuesto se logra determina la valoración de probabilidad de ocurrencia y el nivel de impacto de las vulnerabilidades de los activos de TI?			
10	¿El modelo propuesto establece con efectividad la valoración de niveles de riesgos TI?			

11	¿El modelo propuesto permite determinar la priorización del riesgo dentro de un mapa de calor que facilite una correcta toma de decisiones?			
12	¿Las opciones de tratamiento de riesgo del modelo propuesto permite tomar acciones correctivas ante un riesgo?			
13	¿El modelo propuesto ayuda a definir planes de tratamiento para reducir el efecto de los riesgos?			
14	¿El modelo propuesto permite monitorear regularmente los planes de tratamiento de riesgo?			

GUÍA PARA EL DESARROLLO DEL CUESTONARIO

1. **¿A partir del modelo propuesto se puede definir el alcance de la gestión de riesgos?**

   La definición del alcance permite a la organización establecer los procesos comerciales donde se realizará la gestión de riesgos, el cual se encuentra alineado a la estrategia comercial.

   Datos de Entrada:

   - Plan estratégico de la organización.

   Salida:

   - La matriz de definición del alcance.

2. **¿El modelo propuesto permite a la organización establecer el contexto externo e interno en el cual opera la organización?**

   El contexto externo puede incluir el ámbito legal, económico, competitivo y tecnológico que rodea a la organización y que tiene injerencia en la misma.

   El contexto interno son los factores que intervienen en el día a día sobre la gestión de la organización.

   Datos de Entrada para contexto externo:

   - Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT).
   - Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).
   - Instituto Nacional de Defensa Civil (INDECI).
   - Superintendencia de Banca y Seguros del Perú (SBS).
   - Banco Central de Reserva del Perú (BCRP).

- Lista de oportunidades y amenazas.
- Revista de activos tecnológicos (ESAN).

Datos de Entrada para contexto interno:

- Plan Estratégico de la organización.
- Manual de organización y funciones (MOF) de la organización.
- Organigrama de la organización
- Inventario de activos de la organización.

Salida:

- La matriz de contexto externo.
- La matriz de contexto interno.

3. **¿A partir del modelo propuesto se puede identificar los procesos o actividades que apoyan la estrategia comercial de la organización?**

   Es importante identificar los procesos que se desarrollan en los procesos comerciales para obtener una visión general de cada uno de ellos.

   Datos de entrada:

   - Plan estratégico de la organización u otro documento de referencia se similares características.

   Salida:

   - La matriz de identificación de procesos comerciales.

4. **¿En el modelo propuesto se logra identificar los activos de TI que intervienen en los procesos comerciales de la organización?**

   Se identifican los activos de TI que intervienen en los procesos comerciales para garantizar la gestión eficiente del tiempo en las áreas de la organización.

Datos de entrada:

- Lista de activos de TI que intervienen en los procesos comerciales de la organización.

Salida:

- La matriz de identificación de activos de TI.

5. **¿El modelo propuesto permite a la organización clasificar los de activos de TI?**

   Tomando las recomendaciones de la metodología Magerit v3.0 se clasificaron los activos de TI como procesos de negocio, servicios, software, hardware y soporte de información.

   Datos de entrada:

   - Lista de activos de TI que intervienen en los procesos comerciales de la organización.

   Salida:

   - La matriz de identificación de activos de TI.

6. **¿La valoración de criterios de los activos de TI como confidencialidad, integridad y disponibilidad en el modelo propuesto, se ajusta a la realidad de la organización?**

   El modelo propuesto propone criterios de valoración de activos de TI, considerando el grado de importancia que tienen para la organización.

   Datos de entrada:

   - La matriz de identificación de activos de TI.

   Salida:

   - La matriz de valoración de activos de TI.

7. **¿En el modelo propuesto se identifican las amenazas y vulnerabilidades a las que están expuestos los activos de TI?**

   Es importante determinar las amenazas y vulnerabilidades a los cuales están expuestos los activos de TI que intervienen en los procesos comerciales

   Datos de entrada:

   - La matriz de identificación de activos de TI.

   Salida:

   - La matriz de identificar amenazas.
   - La matriz de identificar vulnerabilidades.

8. **¿En el modelo propuesto se puede identificar, clasificar y analizar los diferentes escenarios de riesgos de TI, en la organización?**

   El modelo propuesto permite a la organización identificar, clasificar y analizar los diferentes escenarios de riesgos TI y realizar una valoración de los mismos.

   Datos de entrada:

   - La matriz de identificar vulnerabilidades.

   Salida:

   - La matriz de análisis de los riesgos.

9. **¿En el modelo propuesto se logra determina la valoración de probabilidad de ocurrencia y el nivel de impacto de las vulnerabilidades de los activos de TI?**

   El modelo propuesto propone dos tablas para realizar la valoración de probabilidad de ocurrencia de ocurrir un evento y la valoración de

impacto que tendría el evento en los procesos comerciales de la organización.

Datos de entrada:

- La matriz de identificar vulnerabilidades.

Salida:

- La matriz de análisis de los riesgos.

10. **¿El modelo propuesto establece con efectividad la valoración de niveles de riesgos TI?**

    En el modelo se proponen 3 niveles de riesgos alto, moderado, bajo.

    Datos de entrada:

    - La matriz de identificar vulnerabilidades.

    Salida:

    - La matriz de análisis de los riesgos.

11. **¿El modelo propuesto permite determinar la priorización del riesgo dentro de un mapa de calor que facilite una correcta toma de decisiones?**

    De acuerdo a la probabilidad de ocurrencia y el nivel de impacto de un determinado evento el modelo permite determinar la prioridad del riesgo dentro de un mapa de calor.

    Datos de entrada:

    - La matriz de análisis de los riesgos.

    Salida:

    - La matriz de valoración del riesgo.

12. **¿Las opciones de tratamiento de riesgo del modelo propuesto permite tomar acciones correctivas ante un riesgo?**

    El modelo propuesto permite determinar estrategias para el tratamiento de cada escenario de riesgo, tomando como referencia el marco COBIT, el cual define como posibles estrategias: evitar, transferir – compartir, mitigar y aceptar.

    Datos de entrada:

    - La matriz de valoración del riesgo.

    Salida:

    - La matriz de plan de tratamiento de riesgos.

13. **¿El modelo propuesto ayuda a definir planes de tratamiento para reducir el efecto de los riesgos?**

    El modelo propone planes para tratar el riesgo, donde se especifica la manera en la que se implementarán las opciones para el tratamiento y propone una estrategia de respuesta al riesgo reduciendo la probabilidad de ocurrencia y el impacto en los procesos comerciales.

    Datos de entrada:

    - La matriz de valoración del riesgo.

    Salida:

    - La matriz de plan de tratamiento de riesgos.

14. **¿El modelo propuesto permite monitorear regularmente los planes de tratamiento de riesgo?**

    El modelo permite realizar un seguimiento continuo y revisión periódica de los planes de tratamiento.

    Datos de entrada:

- La matriz de plan de tratamiento de riesgos.

Salida:

- La matriz de Seguimiento y revisión periódica del plan de tratamiento para cada riesgo.

Anexo 12: Resultado de Cuestionario para medir el nivel de utilidad del modelo propuesto en la empresa 01

RESULTADO DE CUESTIONARIO PARA MEDIR EL NIVEL DE UTILIAD DEL MODELO PROPUESTO EN LA EMPRESA 01

N°	PREGUNTA	JEFE DE TI	PESO
1	¿A partir del modelo propuesto se puede definir el alcance de la gestión de riesgos?	SI	2
2	¿El modelo propuesto permite a la organización establecer el contexto externo e interno en el cual opera la organización?	SI	2
3	¿A partir del modelo propuestos se puede identificar los procesos o actividades que apoyan la estrategia comercial de la organización?	SI	2
4	¿En el modelo propuesto se logra identificar los activos de TI que intervienen en los procesos comerciales de la organización?	SI	2
5	¿El modelo propuesto permite a la organización clasificar los de activos de TI?	SI	0.5
6	¿La valoración de criterios de los activos de TI como confidencialidad, integridad y disponibilidad en el modelo propuesto, se ajusta a la realidad de la organización?	SI	0.5
7	¿En el modelo propuesto se identifican las amenazas y vulnerabilidades a las que están expuestos los activos de TI?	SI	0.5
8	¿En el modelo propuesto se puede identificar, clasificar y analizar los diferentes escenarios de riesgos de TI, en la organización?	SI	1
9	¿En el modelo propuesto se logra determina la valoración de probabilidad de ocurrencia y el nivel de impacto de las vulnerabilidades de los activos de TI?	SI	0.5
10	¿El modelo propuesto establece con efectividad la valoración de niveles de riesgos TI?	SI	0.5
11	¿El modelo propuesto permite determinar la priorización del riesgo dentro de un mapa de calor que facilite una correcta toma de decisiones?	SI	0.5
12	¿Las opciones de tratamiento de riesgo del modelo propuesto permite tomar acciones correctivas ante un riesgo?	SI	2
13	¿El modelo propuesto ayuda a definir planes de tratamiento para reducir el efecto de los riesgos?	SI	2
14	¿El modelo propuesto permite monitorear regularmente los planes de tratamiento de riesgo?	SI	4