UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

MODELO BASADO EN METODOLOGÍAS DE GESTIÓN DE RIESGOS DE TI PARA CONTRIBUIR EN LA MEJORA DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN EMPRESAS DEL SECTOR AGROINDUSTRIAL DE 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

JOSÉ CARLOS BANDA SANTISTEBAN

ASESOR

MTRO. GREGORIO MANUEL LEÓN TENORIO

Chiclayo, 2019

DEDICATORIA

A mis padres por ser mi pilar fundamental y haberme apoyado incondicionalmente.

EPÍGRAFE

Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber.

Albert Einstein

AGRADECIMIENTOS

A mi asesor Mtro. Gregorio Manuel León Tenorio y la Mtro. María Ysabel Arangurí García, por el apoyo brindado durante el desarrollo del proyecto de tesis.

Al Dr. Ernesto Karlo Celi Arévalo, por sus recomendaciones basadas en su experiencia profesional, que permitieron terminar satisfactoriamente este proyecto.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Las empresas agroindustriales de la región Lambayeque constantemente sufren incidentes que comprometen la seguridad de sus activos de información. Según un diagnóstico realizado a una muestra de estas empresas, entre los incidentes más comunes tenemos la paralización de procesos, la pérdida de información, la infección y propagación de virus informáticos.

La presente investigación brinda una propuesta de solución frente a los escenarios de riesgo a los que se encuentran expuestos los activos de información. Para ello, se ha realizado el análisis de conceptos, estándares y metodologías relacionados con la gestión de riesgos, los mismos que al ser adaptados al contexto de las empresas agroindustriales proporcionan las guías necesarias para reducir el nivel de riesgo.

El objetivo general formulado para la investigación: contribuir en la mejora de la seguridad de los activos de información desarrollando un modelo basado en metodologías de gestión de riesgos de TI para las empresas del sector agroindustrial de la región Lambayeque.

El modelo propuesto ha sido validado a través del juicio de expertos midiendo su confiabilidad aplicando el alfa de Cronbach y la concordancia de la evaluación de expertos con base en Kendall.

El modelo validado se aplicó en una empresa agroindustrial de la región como estudio de caso. Se realizó la identificación de algunos escenarios de riesgo, así como el cálculo y la clasificación del nivel de riesgo, según los criterios de aceptación definidos. Además, se propusieron proyectos para mitigar los riesgos que no se encontraban en un nivel aceptable para la empresa.

Palabras clave: Gestión de riesgos, activos de información, escenario de riesgo, empresas agroindustriales, región Lambayeque.

ABSTRACT

Agroindustrial companies in Lambayeque region constantly suffer incidents which compromise the security of their information assets. According to a diagnosis taken from a sample of these companies, the most common incidents are the paralysis of processes, loss of information, infection and spread of computer viruses.

This research provides a solution proposal facing risk scenarios where assets are exposed. For this, the analysis of concepts, standards and methodologies related to risk management has been carried out, the same as those ones which have been adapted to the context of agribusiness companies, provide the necessary guidelines to reduce the level of risk.

The general objective formulated for research: to contribute to the improvement of the security of information assets by developing a model based on IT risk management methodologies for companies in the agribusiness sector of Lambayeque region.

The proposed model has been validated through expert judgment by measuring its reliability and applying Cronbach's alpha and the concordance of the Kendall-based expert evaluation.

The validated model was applied in an agribusiness company in the region as a case study. Some risk scenarios were identified, as well as the calculation and classification of the level of risk, according to defined acceptance criteria. In addition, projects were proposed to diminish risks which were not at an acceptable level to the company.

Keywords: Risk management, information assets, risk scenario, agribusiness companies, Lambayeque region.

INTRODUCCIÓN

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) [1] sostiene que las empresas tienen como objetivo de gobierno la creación de valor, para lo cual, deben lograr la optimización de la gestión del riesgo. Esto implica, que los riesgos relacionados con sus activos de información sean gestionados adecuadamente, asegurando así, que el impacto sobre la empresa no exceda los niveles de apetito y tolerancia establecidos.

El Consejo Superior de Administración Electrónica (CSAE) [2] afirma que gestionar el riesgo es de vital importancia para el gobierno de las empresas, en especial aquellos riesgos que se originan al utilizar las tecnologías de la información (TI), puesto que pueden afectar a los objetivos y metas organizacionales.

Ramírez y Ortiz [3] argumentan que la intensificación del uso de las TI en las empresas, las han convertido en blancos de ataques y vías para perpetuarlos. La gestión adecuada de estos activos, permitirá equilibrar los beneficios y riesgos provenientes del uso de estas tecnologías. En consecuencia, es necesario crear y adaptar continuamente medios y métodos para conservar la seguridad de los activos de información.

ESET [4] ha recopilado información de ejecutivos, técnicos y gerentes que trabajan en más de 2500 empresas de 15 países de la región, con la finalidad de conocer qué acciones se están realizando para proteger los activos de información en las empresas de Latinoamérica, obteniendo como resultado que al menos tres de cada cinco empresas en la región sufrieron, por lo menos, un incidente de seguridad. Por otro lado, se evidencia que cada vez son menos las empresas que no cuentan con al menos un control básico de seguridad, sin embargo, estos controles no son gestionados correctamente.

A continuación, se presentan algunos incidentes que demuestran el impacto que pueden tener ciertos escenarios de riesgo sobre la empresa:

En 2012, Knight Capital, empresa dedicada al comercio de acciones bursátiles, presentó algunos errores en el nuevo software que usaba para vincularse con la plataforma de la Bolsa de Valores de Nueva York, realizándose la compra de acciones a un precio alto y la venta a un precio menor. Estas transacciones duraron alrededor de 45 minutos, lo que significó la pérdida de $ 440 millones dejando así a la empresa al borde de la quiebra [5].

En 2016, Delta Airlines, aerolínea comercial estadounidense, sufrió la caída de su sistema informático, lo que generó el retraso y la cancelación de cientos de vuelos durante varios días, dejando cuantiosas pérdidas económicas debido a que se realizaron reembolsos y obsequiaron cupones a los pasajeros afectados [6].

En 2016, Tesco Bank, una filial bancaria de la cadena británica de supermercados Tesco, experimentó un ciberataque que comprometió a 40,000 cuentas corrientes de sus clientes, de las cuales alrededor de 9,000 consistieron en el robo de dinero. Debido a esto, Tesco Bank suspendió temporalmente las transacciones de débito en línea y reembolsó alrededor de £ 2.5m a los clientes que se vieron afectados por el fraude [7].

En 2016, Bancolombia, organización financiera colombiana, tuvo algunos problemas con sus plataformas tecnológicas, que afectaron de manera importante el servicio a los clientes y usuarios durante los meses de junio y julio. Debido a ello, la Superintendencia Financiera le impuso una sanción por 840 millones de pesos, en febrero de 2017 [8].

En 2015, Interbank Perú, institución financiera perteneciente al Grupo Intercorp, sufrió la caída de su sistema informático entre el 11 y 16 de diciembre, afectando la disponibilidad de los fondos que los consumidores

mantenían en sus cuentas de ahorro, así como el uso normal de los servicios contratados. En consecuencia, Indecopi sancionó a Interbank con una multa de S/ 76,950 por perjudicar a los clientes [9].

Estos incidentes nos demuestran la importancia de gestionar apropiadamente los riesgos de TI, puesto que, la materialización de estos riesgos puede comprometer la operación y misión de la organización, convirtiéndolos en riesgos corporativos que no solo son de interés del área de TI sino de toda la empresa.

En cuanto a las empresas del sector agroindustrial de la región Lambayeque, constantemente han sufrido incidentes de infección y propagación de virus informáticos, paralización de procesos, pérdida de integridad, confidencialidad y disponibilidad de la información y daños en la infraestructura de red; esto debido a que no se realiza un proceso adecuado de gestión de riesgos de TI para proteger sus activos de información.

A comienzos del 2017, una empresa agroindustrial de la región sufrió un ataque de Ransomware que afectó a las áreas de contabilidad, préstamos y sistemas, viéndose comprometidos informes contables, registros de préstamos a clientes, documentos compartidos y backups de bases de datos. La información perteneciente al área de sistemas había sido respaldada la semana anterior al ataque, por lo que estos archivos pudieron ser recuperados. En cambio, la información del área de contabilidad y préstamos fue pérdida en su totalidad, lo que significó pérdidas económicas debido a los préstamos que no pudieron ser cobrados.

Por lo antes mencionado, el presente proyecto de investigación se formuló la siguiente interrogante: ¿De qué manera la elaboración de un modelo basado en metodologías de gestión de riesgos de TI puede contribuir en la mejora de la seguridad de los activos de información en las empresas del sector agroindustrial de la región Lambayeque? A lo que se planteó la siguiente hipótesis: Con la implementación de un modelo basado en

metodologías de gestión de riesgos de TI se contribuye en la mejora de la seguridad de los activos de información en las empresas del sector agroindustrial de la región Lambayeque.

De la hipótesis se desprende la variable Independiente definida como Modelo Basado en Metodologías de Gestión de Riesgos de TI. Como variable Dependiente se propuso contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque.

El presente proyecto de investigación tiene como propósito contribuir en la mejora de la seguridad de los activos de información desarrollando un modelo basado en metodologías de gestión de riesgos de TI para las empresas del sector agroindustrial de la región Lambayeque, lo cual se planteó evaluar con base en el alcance de los siguientes objetivos específicos:

- Analizar los criterios y métodos utilizados en reconocidas metodologías de gestión de riesgos de TI, con la finalidad de seleccionar los que más se adecuen a las empresas del sector en estudio.
- Proponer el modelo basado en metodologías de gestión de riesgos de TI adaptado para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque.
- Validar la implementación del modelo de gestión de riesgos de TI, adaptado para contribuir en la seguridad de los activos de información en las empresas del sector agroindustrial de la región Lambayeque.
- Validar el modelo de gestión de riesgos de TI mediante juicio de expertos, para determinar su utilidad en las empresas del sector agroindustrial de la región Lambayeque.

La importancia del presente proyecto de investigación se justificó con base en varios aspectos, los cuales se presentan a continuación:

En cuanto a lo económico, una correcta gestión de los riesgos de TI permite reducir los costes generados por el mantenimiento correctivo de los activos de información al materializarse cualquier incidente sobre ellos. Por otro lado, también permite incrementar el nivel de productividad debido a la disminución de los incidentes que paralizan las actividades de los colaboradores.

En cuanto a lo social, se puede contribuir a la mejora de la seguridad de los activos de información de cualquier empresa del sector agroindustrial de la región. Además, permite aumentar el nivel de satisfacción de los clientes y colaboradores al disminuir el número de incidentes que incrementan el tiempo de atención.

En lo tecnológico, se trata de una herramienta con la que toda organización debe contar para incrementar la probabilidad de alcanzar sus objetivos estratégicos, y la cual tiene como finalidad contribuir en la mejora de la seguridad de los activos de información brindando conocimientos acerca del nivel de riesgo al que se encuentran expuestos y cómo gestionarlos oportunamente.

CAPÍTULO I: MARCO TEÓRICO CONCEPTUAL

1. ANTECEDENTES DEL PROBLEMA

En 2011, Ramírez y Ortiz [3] desarrollaron una metodología para gestionar riesgos tecnológicos basados en los estándares ISO 31000, ISO/IEC 27005 y otras metodologías importantes en gestión de riesgos, motivados por la problemática que implica el uso de tecnologías de la información en la empresa. Esta metodología trató los lineamientos de la gestión de riesgos bajo el esquema de una organización integral, permitiendo su inclusión en la gestión de continuidad de negocios como fase de apoyo. Para lo cual se realizó la identificación de dependencias claves, activos y procesos críticos, así como amenazas existentes y futuras.

Este antecedente fue una referencia para la presente investigación, en la medida que sustenta como una metodología de gestión de riesgos de TI permite evitar la paralización de los procesos críticos dentro de una empresa, realizando para ello, la identificación de los activos de información críticos y las amenazas que los rodean para posteriormente ser gestionados de una manera adecuada.

En 2014, Moncayo [10] desarrolló un modelo de evaluación de riesgos, basado en metodologías MAGERIT, OCTAVE y normas NIIF (Normas Internacionales de Información Financiera), orientado a resolver la problemática de empresas del sector automotriz en Ecuador, como Provemovil S.A y Provealquileres S.A, las cuales no han definido modelos formales para realizar una evaluación de riesgos, debido a que consideran que son rigurosas y de alto costo. Los contenidos de estas normas fueron adoptados para completar un ciclo de identificación de activos clasificándolos en servicios, hardware, software, soportes de información y personas, así como la identificación de sus vulnerabilidades. Finalmente, la aplicación del modelo en estas empresas

fue favorable, ya que permitió encontrar debilidades y amenazas con respecto a la vida útil y valores contables de los activos.

Este antecedente proporcionó al presente proyecto de investigación un enfoque interesante con respecto a la utilización de diferentes herramientas, como son MAGERIT y OCTAVE, para identificar y clasificar los distintos activos de la empresa, y el uso de las normas NIIF para la clasificación y valoración contable de activos.

En 2014, Martínez [11] desarrolló una propuesta de implementación de controles de seguridad basado en la norma ISO/IEC 17799 en el Servicio de Administración Tributaria de Huancayo, debido a que los controles físicos, técnicos y administrativos que protegen la infraestructura física y tecnológica, sistemas de información, recursos humanos y financieros que generan y procesan la información, no han sido suficientes para garantizar y mantener los principios básicos de la seguridad de la información. Luego de la implantación de los controles propuestos, que tenían mayor grado de importancia y urgencia, se evidenció la reducción del porcentaje de incidencias.

Con respecto a este antecedente, nos detalló cómo se lleva a cabo el proceso de implementación de controles de seguridad de la norma ISO/IEC 17799 (actualmente ISO/IEC 27005) para reducir la cantidad de incidentes materializados sobre los activos, algo que fue de importancia al presente proyecto de investigación puesto que se propone la utilización de controles para los escenarios de riesgo de las empresas del sector agroindustrial de la región.

En 2014, Amador [12] desarrolló una adaptación de la metodología OCTAVE-S con base en la norma ISO/IEC 27005 para gestionar el riesgo en la seguridad de la información en el proceso de Inscripciones y Admisiones de la Universidad del Cauca en Colombia. Con ayuda de esta metodología se pudo definir una estrategia de protección, así como el

plan de mitigación del riesgo, incluyendo los controles a implantar como parte del tratamiento, con la finalidad de ejecutar el proceso de Inscripciones y Admisiones con un nivel bajo de riesgo. Fueron implantados dos controles sugeridos para el tratamiento del riesgo lo cual disminuyó el riesgo en un 5.63%, por lo que se sugirió la implantación de más controles para obtener un porcentaje de reducción significativo.

Este antecedente aportó al presente proyecto de investigación, un enfoque para adaptar metodologías de gestión de riesgos a un sector empresarial específico, algo que resultó de gran utilidad, ya que en la presente investigación se realizó una adaptación de metodologías similares, para adecuarse así a los procesos y activos de información de las empresas del sector agroindustrial.

En 2015, Molina [13] desarrolló un plan de gestión de riesgos tecnológicos siguiendo la metodología MAGERIT en el centro que administra y brinda los servicios de red y sistemas de la Escuela Superior Politécnica del Litoral en Ecuador. Como resultado de la evaluación de los activos de información se demostró que los niveles de riesgos presentes, afectaban directamente a la confidencialidad, integridad y disponibilidad de la información. Además, también se detectó que las protecciones físicas se han implementado de forma correcta, en cambio, las protecciones lógicas aun requerían ser analizadas, desarrolladas y gestionadas. Finalmente se desarrolló un plan de seguridad que consta de una política de seguridad y un plan de ejecución que necesitó la participación del personal de varias áreas.

En este antecedente se dejó claro que la gestión de riesgos requiere de la participación y el compromiso de todas las áreas de la empresa para que de esta manera los diferentes tipos de controles implementados funcionen adecuadamente, algo que fue de utilidad a la presente

investigación para concientizar al personal de las empresas sobre la relevancia de su colaboración en el proceso de gestión de riesgos de TI.

En 2017, Arévalo [14] desarrolló una metodología para la gestión de riesgos de tipo tecnológico con enfoque en la mejora continua basándose en los estándares ISO 31000 e ISO/IEC 27005; además incorporaron recomendaciones, conceptos y buenas prácticas de otras guías y metodologías tales como MAGERIT, ISO 27001, ISO 27002 e ITIL v3. Esta metodología propuesta fue aplicada en el departamento de producción de una empresa industrial de alimentos en Ecuador. Luego de la aplicación de esta metodología, para todos los riesgos identificados, se planteó exitosamente un plan de tratamiento de riesgos. Aunque esta metodología se realizó y evaluó en una empresa industrial de alimentos, también podría servir en empresas industriales de diversos tipos.

Este antecedente fue relevante para el presente proyecto de investigación, por cómo se implementa un proceso de gestión de riesgos, basado en estándares y metodologías, en empresas pertenecientes al sector industrial.

2. BASE TEÓRICA CONCEPTUAL

2.1. Gestión

Según ISACA [15, p. 91], el término gestión:

> … incluye el uso juicioso de medios (recursos, personas procesos, prácticas, etc.) para conseguir un fin identificado. Es un medio o instrumento mediante el cual el grupo que gobierna consigue un resultado u objetivo. La gestión es responsable de la ejecución dentro de la dirección establecida por el grupo que gobierna. La gestión se refiere a las actividades operacionales de planificación, construcción, organización y control que alinean con la dirección que establece el grupo que gobierna y la información sobre dichas actividades.

De lo anterior se concluye que la gestión es una herramienta que permite al gobierno de las organizaciones realizar actividades de planificación, construcción, organización y control con la finalidad de lograr sus objetivos.

2.2. Riesgo

La Organización Internacional de Estandarización (ISO) [16, p. 1] define el riesgo como: "El efecto de la incertidumbre sobre los objetivos".

El CSAE [2, p. 9] lo define como: "La estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización".

Según Caralli, Stevens, Young y Wilson [17, p. 53] el riesgo es: "La posibilidad de sufrir daño o pérdida. Se refiere a una situación en la que una persona puede hacer algo indeseable o una ocurrencia natural puede causar un resultado indeseable, lo que resulta en un impacto o consecuencia negativa".

De acuerdo a las definiciones anteriores se puede concluir que el riesgo es la posibilidad de pérdida debido a la acción de una amenaza, impactando de forma negativa sobre los objetivos.

2.3. Gestión de riesgos

ISO [16, p. 1] define la gestión de riesgos como: "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo".

Según el Instituto Nacional de Estándares y Tecnología (NIST) [18, p. 6], la gestión del riesgo es:

> … una actividad compleja y multifacética que requiere la participación de toda la organización, desde los principales líderes / ejecutivos que proporcionan la visión estratégica y las metas y objetivos de más alto nivel para la organización; a líderes de nivel medio que planifican, ejecutan y administran proyectos; a personas en las líneas de frente que operan los sistemas de información que apoyan las misiones / funciones de negocio de la organización.

ISACA [15, p. 91], afirma que la gestión de riesgos: "Requiere reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo y/o transfiriendo el riesgo, para gestionarlo en el contexto del apetito de riesgo de una empresa".

Analizando los conceptos previos se concluye que la gestión de riesgos comprende actividades de identificación, evaluación, tratamiento y control de los riesgos, de tal manera que se mantenga dentro de los límites tolerables que la empresa ha impuesto. Además, se necesita de la participación de todos los niveles organizacionales desde los líderes ejecutivos hasta el personal operativo.

2.4. Seguridad

El Parlamento Europeo [19, p. 5], define la seguridad como:

> … la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

De acuerdo con lo anterior, puede definirse a la seguridad como la capacidad de los activos de información de resistir los accidentes o acciones ilícitas o malintencionadas que puedan comprometerlos.

2.5. Activo

Para el CSAE, los activos: "Son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización". [2, p. 19].

Según Caralli, Stevens, Young y Wilson [17, p. 34], un activo: "Es algo de valor para la empresa. Los activos son utilizados por las organizaciones para alcanzar los objetivos, proporcionar un retorno de la inversión y generar ingresos".

El Instituto Nacional de Ciberseguridad de España [20, p. 5] , define a un activo como: "Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. Su protección es el fin último de la gestión de riesgos".

Según las definiciones dadas anteriormente, un activo es un elemento de valor para la organización, el cual tiene como propósito contribuir a la consecución de sus objetivos. Además, la gestión de riesgos debe estar enfocada en la protección de estos activos.

2.6. Activo de Información

Según Caralli, Stevens, Young y Wilson [17, p. 34], un activo de información se define como:

> … la información o los datos que son de valor para la organización, incluida la información como los registros del paciente, la propiedad intelectual o la información del cliente. Estos activos pueden existir en forma física (en papel, CD u otros medios) o electrónicamente (almacenados en bases de datos, en archivos, en computadoras personales).

De acuerdo a la definición anterior, se concluye que los activos de información están conformados por los datos e información que tienen valor para la organización y que pueden encontrarse en forma física o electrónica. Estos activos dan soporte a los diferentes procesos de la organización.

2.7. Activo tecnológico / Activo de TI

Según Caralli, Stevens, Young y Wilson [17, p. 35], los activos tecnológicos describen: "Contenedores electrónicos en los que se almacenan, transportan o procesan los activos de información. Estos activos generalmente incluyen hardware, software, sistemas de aplicaciones, servidores y redes".

Según el concepto anterior, se puede definir a los activos tecnológicos como aquellos elementos electrónicos que almacenan, transportan o procesan información o datos importantes para la organización.

2.8. ISO 31000:2018

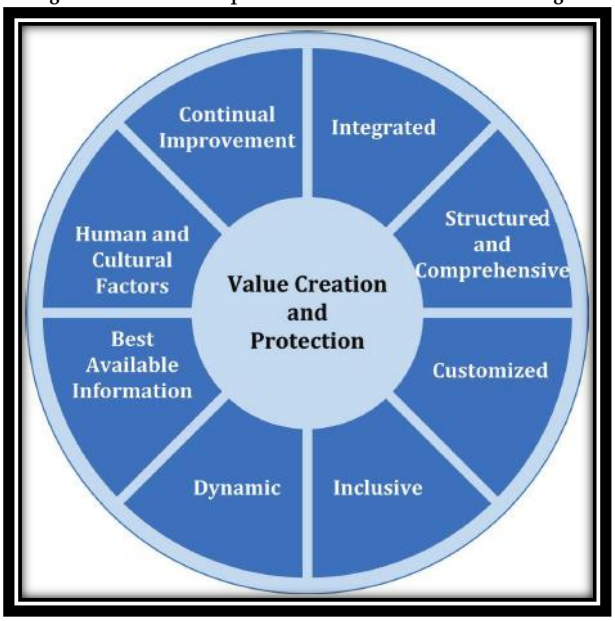
ISO [16] ha desarrollado esta norma para proporcionar directrices sobre la gestión del riesgo que enfrentan las empresas, pudiendo ser personalizadas para cualquier empresa y su contexto.

ISO 31000:2018 se encuentra estructurado de la siguiente manera:

Principios

Estos principios básicos nos orientan acerca de las características que debe presentar una gestión de riesgos efectiva y eficiente, y deben ser considerados al establecer el marco y los procesos de gestión de riesgos de la organización.

Figura 1: Principios de Gestión de Riesgos



Fuente: ISO 31000:2018

La gestión eficaz del riesgo se puede explicar de la siguiente manera.

a) Integrado: Es parte integral de todas las actividades de la organización.
b) Estructurado y comprensivo: Su enfoque estructurado y comprensivo contribuye a lograr resultados consistentes y comparables.
c) Personalizado: El marco y el proceso de gestión de riesgos son personalizados y proporcionales al contexto de la organización en relación con sus objetivos.

d) Inclusivo: Permite tener en cuenta los conocimientos, puntos de vista y percepciones de los stakeholders, a través de la participación adecuada y oportuna de los mismos.
e) Dinámico: Anticipa, detecta, reconoce y responde de manera apropiada y oportuna a los cambios que pueden presentar los riesgos de acuerdo al contexto de la organización.
f) La mejor información disponible: Está basada en información histórica y actual, así como en las expectativas futuras. La información debe ser clara y oportuna, y estar disponible para los stakeholders relevantes.
g) Factores humanos y culturales: Es influenciada por el comportamiento humano y la cultura organizacional.
h) Mejora continua: Mejora continuamente a través del aprendizaje y la experiencia.

Marco de Referencia

Tiene como objetivo ayudar a la organización a integrar la gestión de riesgos en actividades y funciones significativas. El desarrollo del marco abarca la integración, el diseño, la implementación, la evaluación y la mejora de la gestión de riesgos en toda la organización.

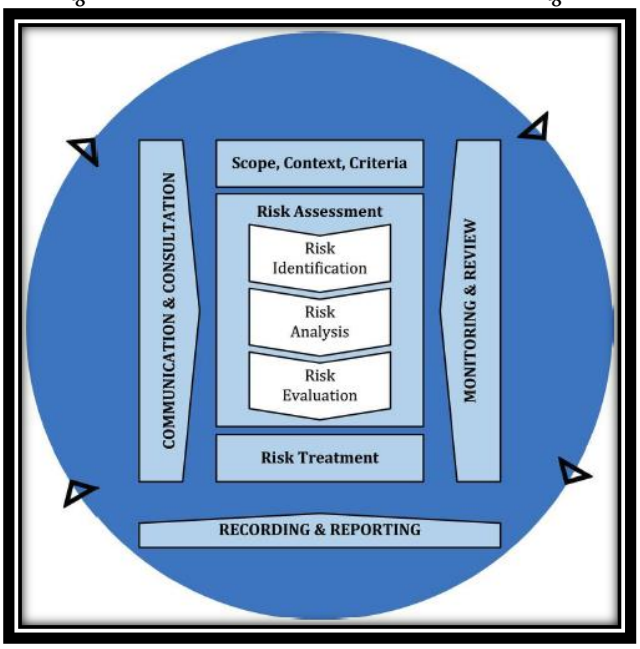
Figura 2: Marco de Gestión de Riesgos

Fuente: ISO 31000:2018

Proceso

El proceso de gestión de riesgos incluye la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, estableciendo el contexto y midiendo, tratando, monitoreando, revisando, registrando y reportando los riesgos.

Figura 3: Proceso de Gestión de Riesgos



Fuente: ISO 31000:2018

2.9. ISO/IEC 27005:2011

ISO [21] en su norma ISO / IEC 27005:2011 proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en ISO / IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Esta norma es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, empresas sin fines de lucro) que pretenden gestionar los riesgos que podrían comprometer la seguridad de la información.

Proceso

Consiste en el establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación y consulta del riesgo, y supervisión y revisión del riesgo.

Este proceso puede ser iterativo para la evaluación del riesgo y / o actividades de tratamiento del riesgo. Un enfoque iterativo para realizar la evaluación del riesgo puede aumentar la profundidad y el detalle de la evaluación en cada iteración.

La efectividad del tratamiento del riesgo depende de los resultados de la evaluación del riesgo.

Se debe tener en cuenta que el tratamiento del riesgo implica un proceso cíclico de:

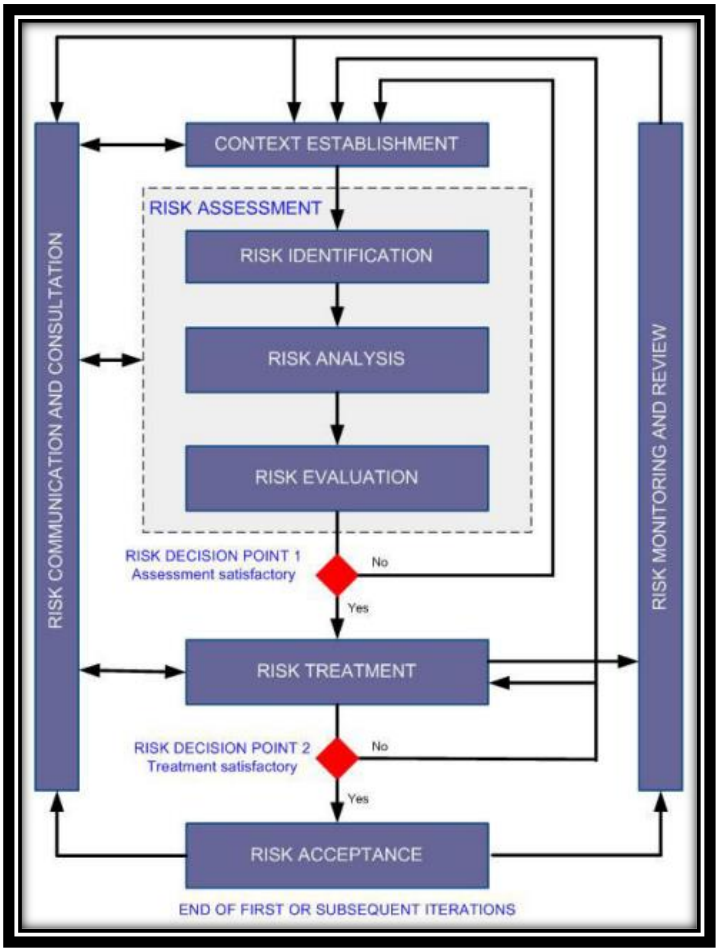
- Evaluar un tratamiento de riesgo;
- Decidir si los niveles de riesgo residual son aceptables;

- Generar un nuevo tratamiento de riesgo si los niveles de riesgo no son aceptables; y
- Evaluar la efectividad de ese tratamiento

Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel aceptable de riesgo residual. En esta situación, puede ser necesaria otra iteración de la evaluación del riesgo con parámetros de contexto modificados (por ejemplo, evaluación de riesgo, aceptación de riesgo o criterios de impacto), si es necesario, seguido de un tratamiento de riesgo adicional.

La actividad de aceptación de riesgos debe garantizar que los riesgos residuales sean explícitamente aceptados por los gerentes de la organización. Esto es especialmente importante en una situación en la que la implementación de controles se omite o se pospone, por ejemplo, debido al costo.

Figura 4: Proceso de Gestión de Riesgos de Seguridad de la Información



Fuente: ISO/IEC 27005:2011

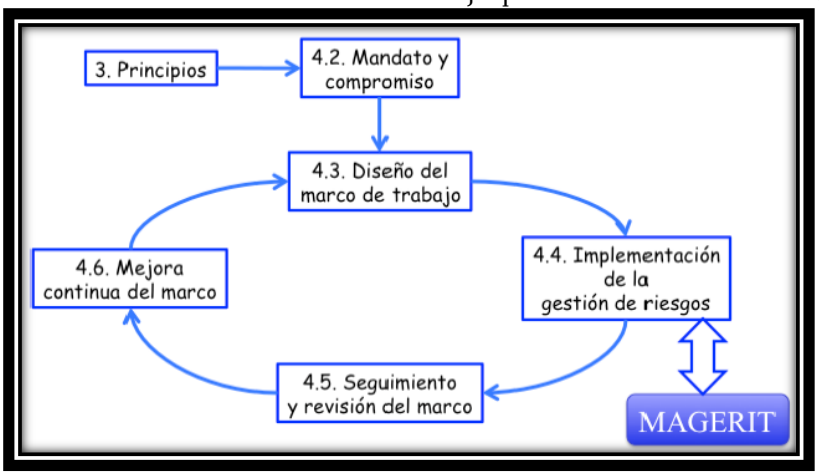
2.10. MAGERIT

Esta metodología elaborada por el CSAE [2], se alinea a ISO 31000 y responde a lo que se denomina "Proceso de Gestión de los Riesgos". Surge como respuesta a la creciente dependencia que tiene la sociedad con respecto a la utilización de las tecnologías de la información y comunicaciones (TIC).

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno

tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 5: ISO 31000 – Marco de Trabajo para la Gestión de Riesgos



Fuente: MAGERIT v3

MAGERIT persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

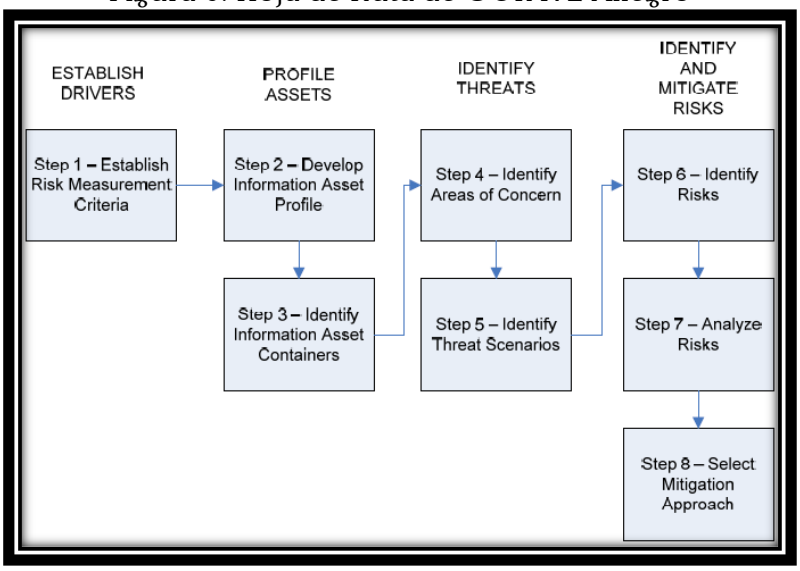
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.11. OCTAVE ALLEGRO

Caralli, Stevens, Young y Wilson [17] han diseñado este enfoque para permitir una amplia valoración del entorno de riesgo operacional de una organización con el objetivo de producir resultados más sólidos sin la necesidad de un amplio conocimiento de evaluación de riesgos.

Este enfoque difiere de los enfoques previos de OCTAVE al enfocarse principalmente en los activos de información en el contexto de cómo se usan, dónde se almacenan, transportan y procesan, y cómo están expuestos a amenazas, vulnerabilidades e interrupciones como resultado. Al igual que los métodos anteriores, OCTAVE Allegro se puede llevar a cabo en un ambiente colaborativo y de estilo taller, y se admite con orientación, hojas de trabajo y cuestionarios. Sin embargo, OCTAVE Allegro también es adecuado para su uso por parte de personas que desean realizar una evaluación de riesgos sin una amplia participación organizacional, experiencia o aportes.

Figura 6: Hoja de Ruta de OCTAVE Allegro

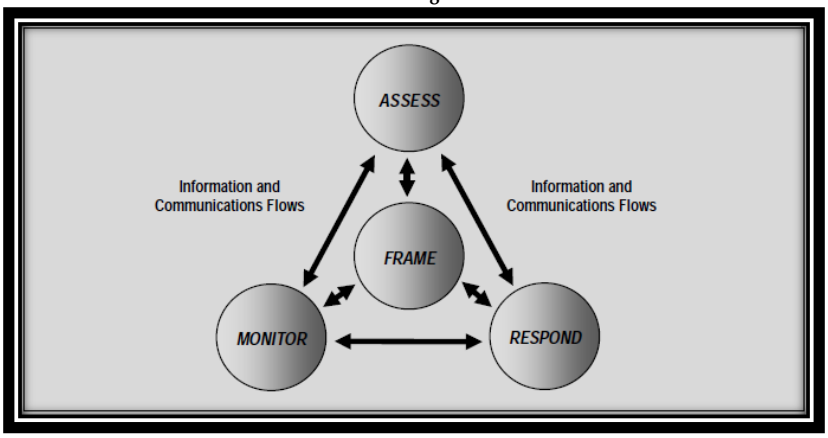


Fuente: Introducing OCTAVE Allegro

2.12. NIST SP 800-30

NIST [22] proporciona esta guía para llevar a cabo cada uno de los pasos del proceso de evaluación de riesgos (es decir, la preparación de la evaluación, la realización de la evaluación, la comunicación de los resultados de la evaluación y el mantenimiento de la evaluación) y cómo las evaluaciones de riesgos y otros procesos de gestión de riesgos se complementan e informan entre sí.

Figura 7: Evaluación del Riesgo dentro del Proceso de Gestión del Riesgo



Fuente: NIST SP 800-30

Esta publicación se centra en el componente de evaluación de riesgos de la gestión de riesgos, que proporciona un proceso paso a paso para las organizaciones sobre como:

- Prepararse para las evaluaciones de riesgos;
- Realizar evaluaciones de riesgo;
- Comunicar los resultados de la evaluación de riesgos al personal clave de la organización; y
- Mantener las evaluaciones de riesgo a lo largo del tiempo.

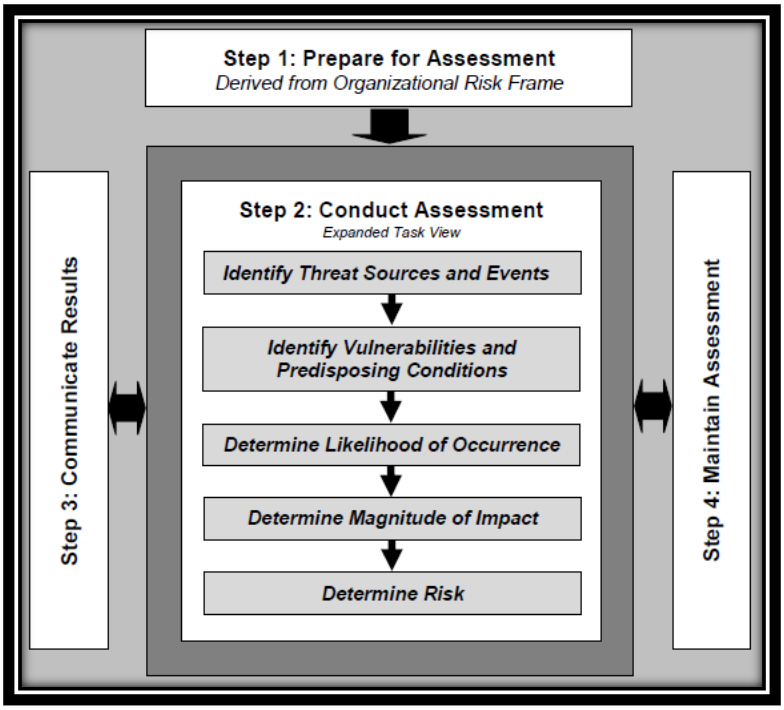
Las evaluaciones de riesgo abordan los posibles impactos adversos para las operaciones y los activos de la organización, los

individuos y otras organizaciones, derivados de la operación y el uso de los sistemas de información y la información procesada, almacenada y transmitida por aquellos sistemas.

El proceso de evaluación de riesgos se compone de cuatro pasos:

(i) Prepararse para la evaluación;
(ii) Realizar la evaluación;
(iii) Comunicar los resultados de la evaluación; y
(iv) Mantener la evaluación.

Figura 8: Proceso de Evaluación del Riesgo



Fuente: NIST SP 800-30

Paso 1: Preparación para la evaluación del riesgo

El objetivo de este paso es establecer un contexto para la evaluación de riesgos. Este contexto está establecido e informado

por los resultados de la etapa de realizar un marco de riesgos del proceso de gestión de riesgos.

Tareas

- Tarea 1-1: Identificar el propósito de la evaluación de riesgos en términos de la información que la evaluación pretende producir y las decisiones que la evaluación pretende respaldar.
- Tarea 1-2: Identificar el alcance de la evaluación de riesgos en términos de aplicabilidad organizacional, marco de tiempo de efectividad y consideraciones de arquitectura / tecnología.
- Tarea 1-3: Identificar las suposiciones y restricciones específicas bajo las cuales se realiza la evaluación de riesgos.
- Tarea 1-4: Identificar las fuentes de información descriptiva, de amenazas, de vulnerabilidad y de impacto que se utilizarán en la evaluación de riesgos.
- Tarea 1-5: Identificar el modelo de riesgo y el enfoque analítico que se utilizará en la evaluación de riesgos.

Paso 2: Realizar la evaluación del riesgo

El objetivo de este paso es producir una lista de riesgos de seguridad de la información que se pueden priorizar según el nivel de riesgo y usar para informar las decisiones de respuesta al riesgo. Para lograr este objetivo, las organizaciones analizan amenazas y vulnerabilidades, impactos y probabilidades, y la incertidumbre asociada con el proceso de evaluación de riesgos.

Tareas

- Tarea 2-1: Identificar y caracterizar las fuentes de amenazas de preocupación, incluidas las características de capacidad, intención y orientación para las amenazas adversas y el rango de efectos para las amenazas no adversas.
- Tarea 2-2: Identificar los eventos de amenaza potenciales, la relevancia de los eventos y las fuentes de amenazas que podrían iniciar los eventos.
- Tarea 2-3: Identificar las vulnerabilidades y las condiciones predisponentes que afectan la probabilidad de que los eventos de amenaza de preocupación resulten en impactos adversos.
- Tarea 2-4: Determinar la probabilidad de que los eventos de amenaza de preocupación resulten en impactos adversos, considerando: (i) las características de las fuentes de amenaza que podrían iniciar los eventos; (ii) las vulnerabilidades / condiciones predisponentes identificadas; y (iii) la susceptibilidad organizativa que refleja las medidas de seguridad / medidas preventivas planificadas o implementadas para impedir tales eventos.
- Tarea 2-5: Determine los impactos adversos de los eventos de amenaza de preocupación, considerando: (i) las características de las fuentes de amenaza que podrían iniciar los eventos; (ii) las vulnerabilidades / condiciones predisponentes identificadas; y (iii) la susceptibilidad que refleja las salvaguardas / contramedidas planeadas o implementadas para impedir tales eventos.
- Tarea 2-6: Determinar el riesgo para la organización de los eventos de amenaza de preocupación, considerando: (i) el impacto que resultaría de los eventos; y (ii) la probabilidad de que ocurran los eventos.

Paso 3: Comunicar y compartir información de evaluación de riesgo

El objetivo de este paso es garantizar que los encargados de tomar decisiones en toda la organización tengan la información apropiada relacionada con el riesgo necesario para informar y guiar las decisiones de riesgos.

Tareas

- Tarea 3-1: Comunicar los resultados de la evaluación de riesgos a los responsables de la toma de decisiones de la organización para respaldar las respuestas de riesgo.
- Tarea 3-2: Compartir la información relacionada con el riesgo producido durante la evaluación del riesgo con el personal de la organización apropiado.

Paso 4: Mantener la evaluación de riesgos

El objetivo de este paso es mantener actualizado el conocimiento específico del riesgo en que incurren las organizaciones. Los resultados de las evaluaciones de riesgos informan las decisiones de gestión de riesgos y guían las respuestas de riesgos.

Tareas

- Tarea 4-1: Realizar un seguimiento continuo de los factores de riesgo que contribuyen a los cambios en el riesgo de las operaciones y los activos de la organización, los individuos.
- Tarea 4-2: Actualizar la evaluación de riesgos existente utilizando los resultados del monitoreo continuo de los factores de riesgo.

CAPÍTULO II: MATERIALES Y MÉTODOS

1. Tipo y nivel de investigación

La presente investigación es Cuantitativa, debido a que se generó una hipótesis que fue probada o desmentida por medios matemáticos y estadísticos. Por su naturaleza corresponde al tipo Cuasi-Experimental puesto que la escogencia de los grupos en los que fue probada la variable independiente fue realizada sin ningún tipo de selección aleatoria o proceso de preselección.

2. Diseño de investigación

Atendiendo a la naturaleza Cuasi experimental de la investigación, el diseño asumido en el siguiente estudio fue el diseño pretest y postest de un solo grupo. En este tipo de diseño se efectúa una observación antes de introducir la variable independiente (Y1) y otra después de su aplicación (Y2).

Secuencia de Tratamiento		
Pretest	Tratamiento	Postest
Y1 Seguridad de los activos de información, antes de aplicar el modelo	X Modelo basado en metodologías de gestión de riesgos de TI	Y2 Seguridad de los activos de información, después de aplicar el modelo

Tabla 1: Secuencia de Tratamiento

3. Población, muestra y muestreo

La población estuvo conformada por empresas del sector agroindustrial cuyas operaciones son realizadas en la región Lambayeque, las cuales son un total de 1,183 empresas según INEI [23].

Para realizar el cálculo de la muestra se utilizó la siguiente fórmula:

$$n = \frac{N * Z_{\alpha}^{2} * p * q}{e^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Donde:

Parámetro	Descripción	Valor
N	Tamaño de la población o universo	1,183
NC	Nivel de confianza	95%
Z	Parámetro estadístico que depende el nivel de confianza (NC)	1.96
e	Error de estimación máximo aceptado	3%
p	Probabilidad de que ocurra el evento estudiado (éxito)	50%
q	Probabilidad de que no ocurra el evento estudiado (1 - p)	50%

Luego de aplicar la formula se obtuvo un tamaño para la muestra (n) de 561 empresas.

Finalmente, por el acceso a la información y diversos criterios de accesibilidad se seleccionaron 4 empresas cuyas características se detallan a continuación:

- **Empresa Agroindustrial 01**

La "Empresa Agroindustrial 01" fue fundada en el año 1999 y se encuentra ubicada en la Car. Panamericana Norte camino a Lambayeque. La misión de la "Empresa Agroindustrial 01" es "brindar productos de calidad, modernizando su industria para obtener una máxima rentabilidad con un alto sentido de responsabilidad y compromiso con el cliente, trabajadores y la sociedad". Así mismo tiene como visión "ser a mediano plazo la empresa líder en la comercialización, procesamiento y abastecimiento de arroz en el Perú".

- **Empresa Agroindustrial 02**

La "Empresa Agroindustrial 02" fue fundada en el año 2003 y se encuentra ubicada en la Car. Panamericana Norte camino a Lambayeque. La misión de la "Empresa Agroindustrial 02" es "integrar toda la cadena productiva y comercial del arroz, innovando y asegurando productos de calidad para beneficio de sus clientes y colaboradores". Así mismo tiene como visión "ser la primera empresa arrocera del Perú".

- **Empresa Agroindustrial 03**

La "Empresa Agroindustrial 03" fue fundada en el año 1994 y se encuentra ubicada en la Car. Panamericana Norte camino a Lambayeque. La misión de la "Empresa Agroindustrial 03" es "buscar la calidad y liderazgo de sus productos, la rentabilidad de su portafolio de negocios y la proyección internacional de sus marcas". Así mismo tiene como visión "ser el portafolio de negocios más rentable del

país, manejando marcas líderes y propias de productos de consumo masivo de alta calidad con distribución a nivel nacional".

- **Empresa Agroindustrial 04**

La "Empresa Agroindustrial 04" fue fundada en el año 1998 y se encuentra ubicada en la Car. Panamericana Norte camino a Lambayeque. La misión de la "Empresa Agroindustrial 04" es "generar valor para sus accionistas, clientes, colaboradores y a la sociedad, otorgando productos de alta calidad; liderando el sector con excelencia en los procesos efectivos con alta tecnología y talento humano comprometido con la excelencia". Así mismo tiene como visión "ser la empresa agroindustrial líder en el mercado nacional e internacional incrementando valor a sus accionistas, clientes, empleados y contribuyendo al progreso del país con confiabilidad, innovación y crecimiento".

4. Criterios de selección

La selección de las empresas que fueron tomadas como muestra para la presente investigación se realizó teniendo en cuenta criterios como:

- Ser empresas que pertenezcan al sector agroindustrial.
- Ser empresas que tienen su sede central en la región Lambayeque.
- Ser empresas con más de 15 años de experiencia en el mercado lambayecano.
- Ser empresas que realicen actividades de procesamiento y comercialización.

- Y por su conveniente accesibilidad y proximidad para el investigador.

5. Técnicas, instrumentos de recolección de datos

- Análisis Documental: Con ayuda de esta técnica se pudo analizar y comparar las metodologías de gestión de riesgos de TI que más se adecuaron al sector empresarial en estudio.
- Modelado: Esta técnica se utilizó para obtener un modelo de gestión de riesgos de TI, basado en las metodologías analizadas previamente, que contribuya en la mejora de la seguridad de los activos de información.
- Cuestionario: Este instrumento fue elaborado en base a criterios relacionados a estándares y metodologías de gestión de riesgos de TI, lo cual permitió realizar el diagnóstico de los activos de información y su exposición al riesgo. Este instrumento fue aplicado a las empresas seleccionadas como muestra de la presente investigación.
- Escala de Likert: Este instrumento fue utilizado para evaluar la opinión de los expertos acerca de la utilidad del modelo de gestión de riesgos de TI propuesto para las empresas del sector agroindustrial de la región.

6. Procedimientos

La recolección de los datos de las encuestas realizadas a los encargados del área de TI se realizó de manera manual, para luego ser procesados a través de la herramienta Excel, por medio de la cual se obtuvieron los análisis y gráficas estadísticas. Además, se utilizó la herramienta SPSS para obtener el coeficiente Alpha de Cronbach y el coeficiente de Concordancia de Kendall para analizar los resultados obtenidos del juicio de expertos.

7. Plan de procesamiento y análisis de datos

- La primera etapa se centró en la revisión de la base teórica relacionada a la gestión de riesgos que fundamentó el desarrollo del modelo propuesto.
- La segunda etapa consistió en el diseño y elección de las herramientas de recolección de información.
- La tercera etapa definió la estructura básica que presentó el modelo propuesto de gestión de riesgos de TI para los activos de información.
- La cuarta etapa identificó y determinó los diferentes activos de información dentro de la empresa, así como los escenarios de riesgo a los que se encuentran expuestos. A partir de esta información se realizó la validación de la hipótesis.
- La quinta etapa consistió en evaluar la solución propuesta a través de juicio de expertos utilizando como referencia la información recolectada con anterioridad. Por último, se llevó a cabo la redacción del informe final de la investigación.

8. Consideraciones éticas

- No se utilizaron ideas, palabras o resultados de otras personas sin otorgarles el reconocimiento que se merecen.
- No fueron creados datos ficticios.
- No se manipularon datos o procedimientos experimentales.
- Se tuvo el consentimiento informado de los participantes.
- Se protegió la identidad de los participantes.
- No se provocó actitudes que condicionen las respuestas de los participantes.

CAPÍTULO III: DISCUSIÓN Y RESULTADOS

I. DIAGNÓSTICO DEL SECTOR

En esta sección se realizó una descripción de las empresas del sector agroindustrial que fueron seleccionadas para realizar el diagnóstico de la situación con respecto a la gestión del riesgo de TI.

Las empresas que fueron seleccionadas cuentan con más de 15 años de presencia en el mercado agroindustrial lambayecano y se encuentran ubicadas en la carretera Panamericana Norte camino a Lambayeque. Estas empresas manifestaron que tienen como misión brindar productos de calidad buscando siempre la mayor rentabilidad para sus negocios. Así mismo, expresaron tener como visión ser la empresa agroindustrial líder en el mercado. El 75% de estas empresas contaba con un área de tecnologías de la información, la cual dependía directamente de la Gerencia General. Sin embargo, ninguna de ellas contaba con personal capacitado para gestionar el riesgo relacionado a las TI.

Para realizar el diagnóstico de la situación del riesgo de TI en empresas del sector agroindustrial en la región Lambayeque, se aplicó un cuestionario dirigido a los encargados de las áreas de tecnologías de la información de las empresas mencionadas anteriormente. La estructura del cuestionario ha sido basada en las actividades de las prácticas de gestión especificadas en el apartado APO12 Gestionar el Riesgo de COBIT5, lo cual proporcionó validez a la herramienta utilizada.

Para mayor detalle acerca del cuestionario ver ANEXO 1.

De acuerdo a los resultados obtenidos del cuestionario aplicado a los encargados de las áreas de TI podemos mencionar lo siguiente:

El 50% de las empresas establecieron parcialmente algunos métodos para identificar, clasificar y analizar datos relacionados al riesgo de TI,

entre los cuales tenemos los reportes obtenidos de un software de gestión de incidencias, reportes de tráfico web y reportes de intentos de ataque por firewall. El 25% realizó un análisis parcial de datos históricos relacionados al riesgo de TI en el sector agroindustrial, utilizando un modo de trabajo de carácter empírico, dado que se ha tomado como referencia experiencias previas del personal del área de TI. El 100% se preocupó en determinar las condiciones existentes cuando ocurrieron los eventos de riesgo, entre las cuales se encontraron el acceso no restringido al contenido web, a las carpetas compartidas y a los puertos USB, falta de capacitación en el uso de los aplicativos, exposición y daños en la infraestructura de red. El 25% establecieron un alcance para realizar el análisis de los riesgos de TI, el cual consistió en los sistemas informáticos propios de la empresa, así como el acceso y tráfico de la red. El 50% construyó al menos un escenario relacionado al riesgo de TI, entre los cuales se tuvieron las pruebas de software, supuestos frente a pérdidas de información e intentos de conexión perimetrales. El 50% realizó una comparación entre el riesgo residual y la tolerancia al riesgo establecida por la empresa. El 25% realizó un análisis costo-beneficio de las opciones de respuesta al riesgo, mediante reuniones entre Gerencia y el personal del área de TI. El 100% estableció controles para mitigar los riesgos de TI como, por ejemplo, herramientas para monitorear el rendimiento de servidores, la actividad web y la actividad de los aplicativos, antivirus y copias de seguridad. El 25% validó los resultados del análisis del riesgo de TI antes de usarlos para la toma de decisiones. El 100% identificó los servicios y recursos de TI que son esenciales para los procesos de negocio de la empresa, entre los cuales tenemos los sistemas institucionales, la base de datos, la infraestructura de red, servidores y equipos de cómputo. El 25% informó los resultados del análisis del riesgo de TI a las partes interesadas. El 50% revisó los resultados obtenidos de las auditorias para decidir si era necesario emprender actividades de análisis del riesgo. El 50% mantuvo un inventario de actividades realizadas para gestionar el

riesgo de TI. El 75% definió proyectos para reducir el efecto del riesgo de TI, entre los cuales tenemos proyectos de software para cumplir con regulaciones legales y proyectos de compra de servidores y firewalls. El 25% documentó parcialmente planes ante la ocurrencia de un evento de riesgo.

Para mayor detalle acerca de los resultados obtenidos del cuestionario aplicado a los encargados de las áreas de TI ver ANEXO 2.

Las gráficas obtenidas a partir de los resultados del cuestionario aplicado las podemos ver en el ANEXO 3.

II. ANÁLISIS DE ESTÁNDARES, MARCOS DE TRABAJO, METODOLOGÍAS RELACIONADAS CON EL TEMA

En esta sección se realizó el análisis de estándares y metodologías para la gestión de riesgos de tecnologías de la información, entre las que tenemos:

- ISO 31000:2018
- ISO/IEC 27005:2011
- MAGERIT 3.0
- OCTAVE ALLEGRO
- NIST SP 800-30

A continuación, se muestra el proceso de análisis de los estándares y metodologías antes mencionadas, tomando como base fundamental el estándar ISO 31000:2018.

1. ALCANCE, CONTEXTO Y CRITERIOS

Según ISO [16], esta fase tiene como propósito "personalizar el proceso de gestión de riesgo, permitiendo una evaluación de riesgos efectiva y un tratamiento de riesgos adecuado".

De acuerdo con NIST [22], el propósito de esta fase es "garantizar que la evaluación produzca la información adecuada y respalde las decisiones previstas".

ISO 31000:2018		ISO/IEC 27005:2011		
Alcance, Contexto y Criterios	Definir el Alcance	**Establecimiento del Contexto**	Alcance y Limites	-
	Contexto Externo e Interno		Contexto Externo e Interno	-
	Definir Criterios del Riesgo		Criterios Básicos	Criterios de Evaluación
				Criterios de Impacto
				Criterios de Aceptación

Tabla 2: Alcance, Contexto y Criterios según ISO 31000:2018 e ISO/IEC 27005:2011

ISO 31000:2018		NIST SP 800-30	
Alcance, Contexto y Criterios	Definir el Alcance	**Prepararse para la evaluación**	Identificar el Alcance
	Contexto Externo e Interno		-
	Definir Criterios del Riesgo		Identificar Suposiciones y Restricciones
			Identificar el Modelo de Riesgo y el Enfoque Analítico

Tabla 3: Alcance, Contexto y Criterios según ISO 31000:2018 y NIST SP 800-30

ISO 31000:2018		MAGERIT 3.0
Alcance, Contexto y Criterios	Definir el Alcance	-
	Contexto Externo e Interno	**Contexto**
	Definir Criterios del Riesgo	**Criterios**

Tabla 4: Alcance, Contexto y Criterios según ISO 31000:2018 y MAGERIT 3.0

1.1. DEFINIR EL ALCANCE

Según ISO [21] , "el alcance del proceso de gestión de riesgos debe definirse para garantizar que todos los activos relevantes se tengan en cuenta en la evaluación de riesgos".

ISO 31000:2018	ISO/IEC 27005:2011	NIST SP 800-30
• 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 • Estrategia (Objetivos estratégicos) **Restricciones que afectan a la organización** • De carácter político • De carácter estratégico • Territoriales • Derivadas del clima económico y político • Estructurales • Funcionales • Relativas al personal • Derivadas del calendario de la organización • Relacionadas con los métodos • De carácter cultural • Presupuestarias **Referencias legislativas y regulatorias** **Restricciones que afectan el alcance** • Derivadas de procesos preexistentes • Técnicas • Financieras • Ambientales • De tiempo • Relacionadas con los métodos • Organizacionales	• Niveles que son abordados en la evaluación. • Partes de la organización que son afectados por la evaluación y como son afectados. • Decisiones que son apoyadas por los resultados de la evaluación. • Cantidad de tiempo que los resultados de la evaluación son relevantes. • Lo que influye en la necesidad de actualizar la evaluación.

Tabla 5: Definir el Alcance según ISO 31000:2018, ISO/IEC 27005:2011 y NIST SP 800-30

1.1.1. La aplicabilidad Organizacional

Según NIST [22], "la aplicabilidad organizacional describe qué partes de la organización se ven afectadas por la evaluación de riesgos y las decisiones basadas en riesgos que resultan de la evaluación".

1.1.2. El Marco de Tiempo de Efectividad

Según NIST [22] , "el marco de tiempo de efectividad determina cuánto tiempo se pueden usar los resultados de las evaluaciones de riesgo para informar legítimamente las decisiones basadas en el riesgo".

1.2. DEFINIR EL CONTEXTO

Según ISO [16], "el contexto del proceso de gestión de riesgos debe establecerse a partir de la comprensión del entorno interno y externo en el que la organización busca definir y lograr sus objetivos".

De acuerdo con el CSAE [2], "El contexto en el que se desarrolla el proceso de gestión de riesgos debe ser objeto de una revisión continua para adaptarse a las circunstancias de cada momento".

1.2.1. Contexto Externo

Según ISO [16], "es el entorno externo en el cual la organización busca alcanzar sus objetivos".

De acuerdo con el CSAE [2], "es el entorno externo en el que opera la organización".

ISO 31000:2018	ISO/IEC 27005:2011	MAGERIT 3.0
• 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. • Relaciones contractuales y compromisos. • Complejidad de redes y dependencias.	• 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. • Relaciones, percepciones y valores de las partes interesadas externas.	• Cultural • Social • Político • Obligaciones, legales, reglamentarias y contractuales • Competencia

Tabla 6: Contexto Externo según ISO 31000:2018, ISO/IEC 27005:2011 y MAGERIT 3.0

1.2.2. Contexto Interno

Según ISO [16], "es el entorno interno en el que la organización busca alcanzar sus objetivos".

De acuerdo con el CSAE [2] , "es el entorno interno en el que se desenvuelve la actividad de la organización".

ISO 31000:2018	ISO/IEC 27005:2011
• Visión, misión y valores. • Gobierno, estructura organizacional, roles y responsabilidades. • Estrategia, objetivos y políticas. • Cultura de la organización. • Estándares, lineamientos y modelos adoptados por la organización. • Capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías). • Datos, sistemas de información y flujos de información. • Las relaciones con las partes interesadas, teniendo en cuenta sus percepciones y valores. • Relaciones contractuales y compromisos.	• Gobierno, estructura organizacional, roles y responsabilidades. • Políticas, objetivos y estrategias que existen para alcanzarlos. • Capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías). • Sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales). • Relaciones, percepciones y valores de las partes interesadas internas. • Cultura de la organización. • Estándares, pautas y modelos adoptados por la organización. • Forma y alcance de las relaciones contractuales.

Tabla 7: Contexto Interno según ISO 31000:2018 e ISO/IEC 27005:2011

1.3. DEFINIR CRITERIOS

Según ISO [16], consiste en:

> … especificar la cantidad y el tipo de riesgo que la organización puede o no asumir, en relación con los objetivos. Además, se definen criterios para evaluar la importancia del riesgo y para respaldar el proceso de toma de decisiones. Los criterios del riesgo son dinámicos y deben revisarse y corregirse continuamente, si es necesario.

De acuerdo a Caralli, Stevens, Young y Wilson [17], "los criterios de evaluación del riesgo se utilizarán para evaluar el efecto de un riesgo sobre los objetivos de misión y empresariales de la organización".

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30
• 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. • Daño a la reputación. • Incumplimientos de requisitos legales, regulatorios o contractuales.	**Actividad 1** Defina un conjunto de medidas cualitativas (criterios de medición de riesgo) contra las cuales podrá evaluar el efecto de un riesgo en la misión y los objetivos comerciales de su organización. Como mínimo, considere las siguientes áreas de impacto: • Reputación / Confianza del cliente • Financiero • Productividad • Seguridad y salud • Multas / Sanciones legales • Área de impacto definida por el usuario **Actividad 2** Priorizar las áreas de impacto de la más importante a la menos importante. La categoría más importante debe recibir la puntuación más alta y la menos importante la más baja.	**Factores de riesgo** • Amenaza • Vulnerabilidad • Impacto • Probabilidad • Condición predisponente **Enfoque de evaluación** • Cuantitativo • Cualitativo • Semicuantitativo **Enfoque de análisis** • Orientado a la amenaza • Orientado al activo / impacto • Orientado a la vulnerabilidad

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30
	Criterios de Aceptación • Pueden incluir umbrales múltiples, con un nivel deseado de riesgo. • 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.		

Tabla 8: Definir Criterios según ISO 31000:2018, ISO/IEC 27005:2011, OCTAVE ALLEGRO y NIST SP 800-30

1.3.1. Criterios de Evaluación

Según NIST [22], "el riesgo y sus factores contribuyentes, pueden evaluarse de varias maneras, incluidas cuantitativa, cualitativamente o semicuantitativamente. Cada enfoque de evaluación de riesgos considerado por las organizaciones tiene ventajas y desventajas".

ISO/IEC 27005:2011

Valores
Insignificante
Muy Bajo
Bajo
Medio
Alto
Muy Alto
Crítico

OCTAVE ALLEGRO

Valores	
Bajo	1
Moderado	2
Alto	3

NIST SP 800-30

Descripciones cualitativas	Valores semicuantitativos	
Muy Bajo	0 – 4	0
Bajo	5 – 20	2
Moderado	21 – 79	5
Alto	80 – 95	8
Muy Alto	96 – 100	10

MAGERIT 3.0

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6 – 8	Alto	Daño grave
3 – 5	Medio	Daño importante
1 – 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Probabilidad de Ocurrencia

MA	Muy Alta	Casi Seguro	Fácil
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Frecuencia de Ocurrencia

MA	100	Muy frecuente	A Diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una Vez al Año
B	1/10	Poco Frecuente	Cada Varios Años
MB	1/100	Muy Poco Frecuente	Siglos

Tabla 9: Escalas de Evaluación según ISO/IEC 27005:2011, OCTAVE ALLEGRO, NIST SP 800-30 y MAGERIT 3.0

1.3.2. Criterios de Análisis

Según NIST [22], los enfoques de análisis:

> … difieren con respecto a la orientación o el punto de partida de la evaluación del riesgo, el nivel de detalle en la evaluación y la forma en que se tratan los riesgos debido a escenarios de amenazas similares. Un enfoque de análisis puede ser: orientado a la amenaza; orientado al activo/impacto; u orientado a la vulnerabilidad.

1.3.3. Criterios de Aceptación

Según ISO [21], "deben definirse criterios o escalas para los niveles de aceptación del riesgo".

2. EVALUACIÓN DEL RIESGO

Según ISO [21], esta fase tiene como propósito:

> … determinar el valor de los activos de información, identificar las amenazas y vulnerabilidades aplicables que existen (o podrían existir), identificar los controles existentes y su efecto en el riesgo identificado, determinar las posibles consecuencias y, finalmente, priorizar los riesgos derivados y clasificarlos en función de los criterios de evaluación de riesgos establecidos en la definición de criterios.

De acuerdo con NIST [22], el propósito de esta fase es "producir una lista de riesgos que se pueden priorizar según el nivel de riesgo y usar para informar las decisiones de respuesta al riesgo".

ISO 31000:2018		ISO/IEC 27005:2011		
Evaluación del Riesgo	Identificación del Riesgo	**Evaluación del Riesgo de SI**	Identificación del Riesgo	Identificación de Activos
				Identificación de Amenazas
				Identificación de Controles Existentes
				Identificación de Vulnerabilidades
				Identificación de Consecuencias
	Análisis del Riesgo		Análisis del Riesgo	Metodologías de Análisis de Riesgos
				Evaluación de Consecuencias
				Evaluación de Probabilidad de Incidentes
				Nivel de Determinación del Riesgo
	Valoración del Riesgo		Valoración del Riesgo	-

Tabla 10: Evaluación del Riesgo según ISO 31000:2018 e ISO/IEC 27005:2011

ISO 31000:2018		OCTAVE ALLEGRO	
Evaluación del Riesgo	Identificación del Riesgo	**Establecer Perfiles de Activos**	Desarrollo de Perfiles de Activos de Información
			Identificación de Contenedores de Activos de Información
		Identificar Amenazas	Identificación de Áreas de Preocupación
			Identificación de Escenarios de Amenaza
		Identificar y Mitigar Riesgos	Identificación de Riesgos
	Análisis del Riesgo		Análisis de Riesgos
	Valoración del Riesgo	-	-

Tabla 11: Evaluación del Riesgo según ISO 31000:2018 y OCTAVE ALLEGRO

ISO 31000:2018		NIST SP 800-30	
Evaluación del Riesgo	Identificación del Riesgo	Realizar la Evaluación	Identificar Fuentes de Amenaza
			Identificar Eventos de Amenaza
			Identificar Vulnerabilidades y Condiciones predisponentes
	Análisis del Riesgo		Determinar la Probabilidad
			Determinar el Impacto
			Determinar el Riesgo
	Valoración del Riesgo	-	-

Tabla 12: Evaluación del Riesgo según ISO 31000:2018 y NIST SP 800-30

ISO 31000:2018		MAGERIT 3.0		
Evaluación del Riesgo	Identificación del Riesgo	Evaluación de los Riesgos (MAR – Método de Análisis de Riesgos)	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
	Análisis del Riesgo		Estimación del Estado de Riesgo	Estimación del Impacto
				Estimación del Riesgo
	Valoración del Riesgo		Caracterización de los Activos	Valoración de los Activos
			Caracterización de las Amenazas	Valoración de las Amenazas
			Caracterización de las Salvaguardas	Valoración de las Salvaguardas

Tabla 13: Evaluación del Riesgo según ISO 31000:2018 y MAGERIT 3.0

2.1. IDENTIFICAR EL RIESGO

Según ISO, "El objetivo de la identificación del riesgo es encontrar, reconocer y describir los riesgos que podrían ayudar o evitar que una organización logre sus objetivos" [16]. "La identificación del riesgo determina qué podría suceder para causar una pérdida potencial y obtener una idea de cómo, dónde y por qué podría ocurrir la pérdida" [21].

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30

• Fuentes de riesgos tangibles e intangibles.
• Causas y eventos.
• Amenazas y oportunidades.
• Vulnerabilidades y capacidades.
• Cambios en el contexto externo e interno.
• Indicadores de riesgos emergentes.
• Naturaleza y valor de los activos y recursos.
• Consecuencias y su impacto en los objetivos.
• Limitaciones de conocimiento y confiabilidad de la información.
• Factores relacionados con el tiempo.
• Sesgos, suposiciones y creencias de los involucrados.
	Identificación de Activos
	Activos Primarios
	• Actividades y procesos del negocio
	• Información
	Activos de Soporte
	• Hardware
	• Software
	• Red
	• Personal
	• Ambientes físicos
	• Estructura organizacional
	
	Identificación de Amenazas
	Tipos de Amenazas
	• Daño físico
	• Eventos naturales
	• Pérdida de servicios esenciales
	• Perturbación debido a la radiación
	• Compromiso de información
	• Fallas técnicas
	• Acciones no autorizadas
	• Compromiso de funciones
	Origen de la Amenaza
	• Hacker, cracker
	• Criminal informático
	• Terrorista
	• Espionaje industrial
	• Insiders (empleados mal capacitados, descontentos,
		Desarrollo de Perfiles de Activos de Información
		
		Identificación de Contenedores de Activos de Información
		Tipos de contenedores internos y externos
		• Técnico
		• Físico
		• Personas
		
		Identificación de Áreas de Preocupación
		
		Identificación de Escenarios de Amenaza
		Propiedades de una amenaza
		• Activo
		• Acceso/Medio (acceso físico, medios técnicos)
		• Actor
		• Motivo (deliberado, accidental)
		• Resultado (revelación, modificación, destrucción, pérdida, interrupción)
		Árboles de amenaza
		• Actores humanos utilizando medios técnicos
			Identificar Fuentes de Amenaza
			Tipos de fuentes de amenaza
			• Adversarial (capacidad, intención, orientación)
			  • Individual
			  • Grupal
			  • Organización
			  • Estado-Nación
			• Accidental
			  • Usuario
			  • Usuario/Administrador Privilegiado
			• Estructural
			  • Equipo de TI
			  • Controles Ambientales
			  • Software
			• Ambiental
			  • Desastres Naturales o Provocados por el Hombre
			  • Evento Natural Inusual
			  • Falla/Corte de Infraestructura
			
			Identificar Eventos de Amenaza
			Tipos de Eventos de Amenaza
			• Adversarial
			• No Adversarial
			Pertinencia de los eventos de amenaza
			• Confirmado
			• Esperado
			• Anticipado

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30

	maliciosos, negligentes, deshonestos o despedidos)
	
	Identificación de Controles existentes
	• Revisión de documentos sobre controles
	• Verificar con personas responsables y usuarios
	• Revisión de resultados de auditorias
	Identificación de Vulnerabilidades
	Tipos de Vulnerabilidades
	• Hardware
	• Software
	• Red
	• Personal
	• Ambientes físicos
	• Organizacional
	
	Identificación de las Consecuencias
	Directas
	• El valor financiero del reemplazo del (parte del) activo perdido.
	• El costo de adquisición, configuración e instalación del nuevo activo o respaldo.
		• Actores humanos utilizando el acceso físico
		• Problemas técnicos
		• Otros problemas
		
		Identificación de Riesgos
		Área de Impacto
		• Reputación
		• Financiero
		• Productividad
		• Seguridad y Salud
		• Multas / Legal
			• Previsto
			• Posible
			• N/A (No Aplicable)
			
			Identificar Vulnerabilidades y Condiciones Predisponentes
			Tipos de Vulnerabilidades
			• Sistemas de Información Organizacionales
			  • Hardware
			  • Software
			  • Firmware
			  • Controles Internos
			  • Procedimientos de Seguridad
			• Entornos de Operación de los Sistemas
			  • Gobierno Organizacional
			  • Relaciones Externas
			  • Procesos de misión / negocio
			  • Arquitectura Empresarial
			  • Arquitectura de Seguridad de la Información
			Tipos de Condiciones Predisponentes
			• Información Relacionada
			• Técnico
			• Operacional / Ambiental

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30
	• El costo de las operaciones suspendidas debido al incidente hasta que se restaure el servicio proporcionado por el (los) activo(s). • El impacto resulta en un incumplimiento de seguridad de la información. Indirectas • Costo de oportunidad. • El costo de las operaciones interrumpidas. • Posible uso indebido de la información obtenida a través de un incumplimiento de seguridad. • Violación de obligaciones legales o regulatorias. • Violación de códigos de conducta ética.		

Tabla 14: Identificar el Riesgo según ISO 31000:2018, ISO/IEC 27005:2011, OCTAVE ALLEGRO y NIST SP 800-30

2.1.1. Identificación de Activos

Según ISO [21], "los activos dentro del alcance establecido deben identificarse".

De acuerdo con el CSAE [2], "identifica los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados".

Según Caralli, Stevens, Young y Wilson [17], "se identifican y perfilan los activos que son el foco de la evaluación de riesgos y se identifican los contenedores de activos".

ISO/IEC 27005:2011	MAGERIT 3.0

• **Activos Primarios**
  o Actividades y procesos del negocio
  o Información
• **Activos de Soporte**
  o Hardware
  o Software
  o Redes
  o Personal
  o Ambientes físicos
  o Estructura organizacional
	• Activos Esenciales
	  o Información que se maneja
	  o Servicios prestados
	• Servicios internos
	• Equipamiento informático
	  o Aplicaciones (software)
	  o Equipos informáticos (hardware)
	  o Comunicaciones
	  o Soportes de información: discos, cintas, etc.
	• Entorno
	  o Equipamiento y suministros: energía, climatización, etc.
	  o Mobiliario
	• Servicios subcontratados a terceros
	• Instalaciones físicas
	• Personal
	  o Usuarios
	  o Operadores y administradores
	  o Desarrolladores

Tabla 15: Clasificación de Activos según ISO/IEC 27005:2011 y MAGERIT 3.0

2.1.2. Valoración de Activos

Según el CSAE [2], "La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes".

ISO/IEC 27005:2011	NIST SP 800-30	MAGERIT 3.0
• Confidencialidad • Integridad • Disponibilidad • No repudio • Responsabilidad • Autenticidad • Confiabilidad	• Confidencialidad • Integridad • Disponibilidad	• Disponibilidad • Integridad • Confidencialidad • Autenticidad • Trazabilidad

Tabla 16: Dimensiones de la Seguridad según ISO/IEC 27005:2011, NIST SP 800-30 y MAGERIT 3.0

2.1.3. Identificación de Amenazas

Según ISO [21], "las amenazas y sus fuentes deben ser identificadas. Las amenazas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden resultar, por ejemplo, en daños o pérdida de servicios esenciales".

De acuerdo con Caralli, Stevens, Young y Wilson [17], "se debe identificar y documentar las amenazas a los activos, en el contexto de sus contenedores, a través de un proceso estructurado".

ISO/IEC 27005:2011	NIST SP 800-30	MAGERIT 3.0

Tipos de Amenazas
• Daño físico
• Eventos naturales
• Pérdida de servicios esenciales
• Perturbación debido a la radiación
• Compromiso de información
• Fallas técnicas
• Acciones no autorizadas
• Compromiso de funciones
 	
Origen de la Amenaza
• Hacker, cracker
• Criminal informático
• Terrorista
• Espionaje industrial
• Insiders (empleados mal capacitados, descontentos, maliciosos, negligentes, deshonestos o despedidos)
	Tipos de Fuentes de Amenaza
	• Adversarial (capacidad, intención, orientación)
	  ○ Individual
	  ○ Grupal
	  ○ Organización
	  ○ Estado-Nación
	• Accidental
	  ○ Usuario
	  ○ Usuario/Administrador Privilegiado
	• Estructural
	  ○ Equipo de TI
	  ○ Controles Ambientales
	  ○ Software
	• Ambiental
	  ○ Desastres Naturales o Provocados por el Hombre
	  ○ Evento Natural Inusual
	  ○ Falla/Corte de Infraestructura
		Tipos de Amenazas
		• De origen natural
		• Del entorno (de origen industrial)
		• Defectos de las aplicaciones
		• Causadas por las personas de forma accidental
		• Causadas por las personas de forma deliberada

Tabla 17: Clasificación de Amenazas según ISO/IEC 27005:2011, NIST SP 800-30 y MAGERIT 3.0

2.1.4. Identificación de Vulnerabilidades

Según ISO [21], "se deben identificar las vulnerabilidades que pueden ser explotadas a través de amenazas para causar daño a los activos o a la organización".

De acuerdo con NIST [22], "se debe identificar las vulnerabilidades y las condiciones predisponentes que

afectan la probabilidad de que los eventos de amenaza resulten en impactos adversos".

ISO/IEC 27005:2011	NIST SP 800-30
• Hardware • Software • Red • Personal • Ambientes físicos • Organizacional	• Sistemas de Información Organizacionales o Hardware o Software o Firmware o Controles Internos o Procedimientos de Seguridad • Entornos de Operación de los Sistemas o Gobierno Organizacional o Relaciones Externas o Procesos de misión / negocio o Arquitectura Empresarial o Arquitectura de Seguridad de la Información

Tabla 18: Tipos de Vulnerabilidades según ISO/IEC 27005:2011 y NIST SP 800-30

2.1.5. Identificación de Impactos

Según Caralli, Stevens, Young y Wilson [17], "se deben identificar las consecuencias para la organización si se realiza una amenaza, completando la imagen del riesgo. Una amenaza puede tener múltiples impactos potenciales en una organización".

De acuerdo con NIST [22], "la organización describe el impacto adverso en términos del daño potencial causado a las operaciones y los activos de la organización".

Según ISO [21], consiste en:

> … identificar el daño o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción

de una amenaza que explota una determinada vulnerabilidad o conjunto de vulnerabilidades en un incidente de seguridad de la información.

ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30	MAGERIT 3.0
Criterios para evaluar las posibles consecuencias • Violación de la legislación y / o regulación. • Deterioro del rendimiento empresarial. • Pérdida de buena voluntad / efecto negativo en la reputación. • Incumplimiento asociado a la información personal. • Peligro de seguridad personal. • Efectos adversos en la aplicación de la ley. • Incumplimiento de confidencialidad. • Incumplimiento del orden público. • Pérdidas financieras. • Interrupción a las actividades empresariales. • Peligro a la seguridad ambiental	**Áreas de Impacto** • Reputación / Confianza del cliente • Financiero • Productividad • Seguridad y salud • Multas / Sanciones legales • Área de impacto definida por el usuario	**Tipos de Impacto** • Daño a las Operaciones • Daño a los Activos • Daño a los Individuos • Daño a Otras Organizaciones • Daño a la Nación	• Coste de reposición: adquisición e instalación. • Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo. • Lucro cesante: pérdida de ingresos. • Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas. • Sanciones por incumplimiento de la ley u obligaciones contractuales. • Daño a otros activos, propios o ajenos. • Daño a personas. • Daños medioambientales.

Tabla 19: Tipos de Impacto según ISO/IEC 27005:2011, OCTAVE ALLEGRO, NIST SP 800-30 y MAGERIT 3.0

2.1.6. Identificación de Salvaguardas

Según ISO [21]:

> … la identificación de salvaguardas debe realizarse para evitar el trabajo o el costo innecesarios, p. en la duplicación de salvaguardas. Además, al identificar las salvaguardas existentes, se debe realizar una verificación para garantizar que las salvaguardas funcionen correctamente. Si un control no funciona como se espera, esto puede causar vulnerabilidades.

De acuerdo con el CSAE [2], "se debe identificar las salvaguardas convenientes para proteger el sistema".

MAGERIT 3.0
• Protecciones generales u horizontales • Protección de los datos / información • Protección de las claves criptográficas • Protección de los servicios • Protección de las aplicaciones (software) • Protección de los equipos (hardware) • Protección de las comunicaciones • Protección en los puntos de interconexión con otros sistemas • Protección de los soportes de información • Protección de los elementos auxiliares • Seguridad física – Protección de las instalaciones • Salvaguardas relativas al personal • Salvaguardas de tipo organizativo • Continuidad de operaciones • Externalización • Adquisición y desarrollo

Tabla 20: Tipos de Salvaguardas según MAGERIT 3.0

2.2. ANALIZAR EL RIESGO

Según ISO, "El análisis del riesgo implica una consideración detallada de las incertidumbres, las fuentes de riesgo, las consecuencias, la probabilidad, los eventos, los

escenarios, los controles y su efectividad" [16]. "El análisis del riesgo puede llevarse a cabo con diversos grados de detalle, dependiendo de la criticidad de los activos, el alcance de las vulnerabilidades conocidas y los incidentes previos que involucran a la organización" [21].

De acuerdo a Caralli, Stevens, Young y Wilson, "El análisis del riesgo mide cualitativamente el grado en que la organización se ve afectada por una amenaza al calcular una puntuación de riesgo por cada riesgo para cada activo de información" [17].

Según el CSAE [2], "En esta actividad se combinan los descubrimientos de las actividades anteriores para derivar estimaciones del estado de riesgo de la organización. El objetivo es disponer de una estimación fundada de lo que puede ocurrir y de lo que probablemente ocurra".

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30
• 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** Tipos de Metodologías • Cualitativa (bajo, medio, alto) • Cuantitativa • Semicuantitativa Valoración Cualitativa de Activos • Insignificante • Muy bajo • Bajo • Medio • Alto • Muy alto • Crítico Aspectos para la Valoración de Activos • Confidencialidad • Integridad • Disponibilidad • No repudio • Responsabilidad • Autenticidad • Confiabilidad Criterios para evaluar las posibles consecuencias • Violación de la legislación y / o regulación. • Deterioro del rendimiento empresarial.	Tipo de Metodología • Cualitativo Valor de Impacto • Bajo (1) • Moderado (2) • Alto (3) Requerimientos de Seguridad • Confidencialidad • Integridad • Disponibilidad • Otro	**Determinar la Probabilidad** Escala de Evaluación • Muy Bajo / 0-4 / 0 • Bajo / 5-20 / 2 • Moderado / 21-79 / 5 • Alto / 80-95 / 8 • Muy Alto / 96-100 / 10 **Determinar el Impacto** Tipos de Impactos • Daño a las Operaciones • Daño a los Activos • Daño a los Individuos • Daño a Otras Organizaciones • Daño a la Nación Escala de Evaluación • Muy Bajo / 0-4 / 0 • Bajo / 5-20 / 2 • Moderado / 21-79 / 5 • Alto / 80-95 / 8 • Muy Alto / 96-100 / 10 **Determinar el Riesgo** Escala de Evaluación • Muy Bajo / 0-4 / 0 • Bajo / 5-20 / 2 • Moderado / 21-79 / 5 • Alto / 80-95 / 8 • Muy Alto / 96-100 / 10

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	NIST SP 800-30
	• Pérdida de buena voluntad / efecto negativo en la reputación. • Incumplimiento asociado a la información personal. • Peligro de seguridad personal. • Efectos adversos en la aplicación de la ley. • Incumplimiento de confidencialidad. • Incumplimiento del orden público. • Pérdidas financieras. • Interrupción a las actividades empresariales. • Peligro a la seguridad ambiental. **Evaluación de Probabilidad de Incidentes** Enfoques de Evaluación de Riesgos • Matriz con valores predefinidos. • Ranking de amenazas por medidas de riesgo. • Evaluación del valor de la probabilidad y las posibles consecuencias de los riesgos.		

Tabla 21: Analizar el Riesgo según ISO 31000:2018, ISO/IEC 27005:2011, OCTAVE ALLEGRO y NIST SP 800-30

2.3. VALORAR EL RIESGO

Según ISO, "el propósito de la valoración del riesgo es apoyar las decisiones. Esto implica comparar los resultados del análisis del riesgo con los criterios de riesgo establecido para determinar dónde se requieren acciones adicionales" [16]. "Se debe comparar los riesgos estimados con los criterios de evaluación de riesgos definidos durante el establecimiento del contexto. La valoración del riesgo utiliza la comprensión del riesgo obtenida por el análisis del riesgo para tomar decisiones sobre acciones futuras" [21].

De acuerdo con el CSAE [2], "La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes".

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

Tabla 22: Valorar el Riesgo según ISO 31000:2018 e ISO/IEC 27005:2011

3. TRATAMIENTO DEL RIESGO

Según ISO [16], esta fase tiene como propósito "seleccionar e implementar opciones para abordar el riesgo".

De acuerdo con Caralli, Stevens, Young y Wilson [17], "la organización determina cuáles de los riesgos que han identificado requieren mitigación y desarrollan una estrategia de mitigación para esos riesgos".

ISO 31000:2018		ISO/IEC 27005:2011	
Tratamiento del Riesgo	Seleccionar Opciones de Tratamiento del Riesgo	**Tratamiento del Riesgo de SI**	Modificar el Riesgo
			Retener el Riesgo
			Evitar el Riesgo
			Compartir el Riesgo
	Preparar e Implementar Planes de Tratamiento del Riesgo		-

Tabla 23: Tratamiento del Riesgo según ISO 31000:2018 e ISO/IEC 27005:2011

ISO 31000:2018		OCTAVE ALLEGRO	
Tratamiento del Riesgo	Seleccionar Opciones de Tratamiento del Riesgo	**Identificar y Mitigar Riesgos**	Selección de Enfoque de Mitigación
	Preparar e Implementar Planes de Tratamiento del Riesgo		-

Tabla 24: Tratamiento del Riesgo según ISO 31000:2018 y OCTAVE ALLEGRO

ISO 31000:2018		MAGERIT 3.0		
Tratamiento del Riesgo	Seleccionar Opciones de Tratamiento del Riesgo	**Decisión de Tratamiento**	Opciones de Tratamiento del Riesgo	Eliminación
				Mitigación
				Compartición
				Financiación
	Preparar e Implementar Planes de Tratamiento del Riesgo		-	-

Tabla 25: Tratamiento del Riesgo según ISO 31000:2018 y MAGERIT 3.0

ISO 31000:2018	ISO/IEC 27005:2011	OCTAVE ALLEGRO	MAGERIT 3.0
Opciones de Tratamiento del Riesgo • Evitar el riesgo al decidir no comenzar o continuar con la actividad que genera el riesgo. • Asumir o incrementar el riesgo para buscar una oportunidad. • Eliminar la fuente del riesgo. • Cambiar la probabilidad. • Cambiar las consecuencias. • Compartir el riesgo (por ejemplo, a través de contratos, compra de seguros). • Retener el riesgo por decisión informada. **Plan de Tratamiento del Riesgo** • Justificación para la selección de las opciones de tratamiento, incluidos los beneficios esperados que se obtendrán. • Responsables de aprobar e implementar el plan. • Acciones propuestas. • Recursos requeridos, incluidas las contingencias. • Medidas de rendimiento. • Restricciones. • Reporte y monitoreo requeridos. • Cuando se espera que las acciones sean emprendidas y completadas.	**Opciones de Tratamiento del Riesgo** • Modificar el Riesgo • Retener el Riesgo • Evitar el Riesgo • Compartir el Riesgo **Modificar el Riesgo** Restricciones para la Modificación del Riesgo • Restricciones de tiempo • Restricciones financieras • Restricciones técnicas • Restricciones operativas • Restricciones culturales • Restricciones éticas • Restricciones ambientales • Restricciones legales • Facilidad de uso • Restricciones de personal • Restricciones de integración de controles nuevos y existentes	**Enfoques de Mitigación** • Aceptar • Postergar • Mitigar • Transferir	• Aceptación • Eliminación • Mitigación • Compartición • Financiación

Tabla 26: Opciones y Plan de Tratamiento del Riesgo según ISO 31000:2018, ISO/IEC 27005:2011, OCTAVE ALLEGRO y MAGERIT 3.0

3.1. SELECCIONAR OPCIONES DE TRATAMIENTO DEL RIESGO

Según ISO, "el propósito es equilibrar los beneficios potenciales derivados del logro de los objetivos contra los costos, el esfuerzo o las desventajas de la implementación. Estas opciones no son necesariamente excluyentes o apropiadas en todas las circunstancias" [16]. "Las opciones de tratamiento del riesgo deben seleccionarse en función del resultado de la evaluación del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados de estas opciones" [21].

3.1.1. Aceptar el Riesgo

Según ISO [21], "si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no hay necesidad de implementar controles adicionales y se puede retener el riesgo".

De acuerdo con el CSAE [2], "cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección".

3.1.2. Mitigar el Riesgo

Según ISO [21]:

> … el nivel de riesgo debe ser gestionado introduciendo, alterando o eliminando controles para que el riesgo residual pueda ser reevaluado como aceptable. Se debe tener en cuenta los criterios de aceptación del riesgo, así como los requisitos legales, reglamentarios y contractuales, el costo, aspectos técnicos, ambientales y culturales.

De acuerdo con el CSAE [2]:

> … la mitigación del riesgo se refiere a una de dos opciones: (i) reducir la degradación causada por una amenaza (a veces se usa la expresión "acotar el impacto"); (ii) reducir la probabilidad de que una amenaza se materialice. En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas.

3.1.3. Compartir el Riesgo

Según ISO [21], "compartir el riesgo implica la decisión de compartir ciertos riesgos con terceros. El compartir riesgos puede crear nuevos riesgos o modificar los riesgos existentes identificados. Por lo tanto, puede ser necesario un tratamiento de riesgo adicional".

De acuerdo con el CSAE [2]:

> … hay dos formas básicas de compartir riesgo: (i) Riesgo Cualitativo, Se comparte por medio de la externalización de componentes del sistema (Se reparten responsabilidades técnicas y legales); (ii) Riesgo Cuantitativo, Se comparte por medio de la contratación de seguros (El asegurador corre con las consecuencias).

3.1.4. Evitar el Riesgo

Según ISO [21] ,

> … cuando los riesgos identificados se consideran demasiado altos o los costos de implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar la decisión de evitar el riesgo por completo, retirándose de una actividad o conjunto

de actividades planificadas o existentes, o cambiando las condiciones bajo el cual se opera la actividad.

De acuerdo con el CSAE [2]:

> … la eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable. En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la organización. Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma.

3.2. PREPARAR E IMPLEMENTAR PLANES DE TRATAMIENTO DEL RIESGO

Según ISO [16], "El propósito de los planes de tratamiento de riesgos es especificar cómo se implementarán las opciones de tratamiento elegidas, para que los involucrados puedan comprender los acuerdos, y se puede monitorear el progreso en relación con el plan".

4. SEGUIMIENTO Y REVISIÓN

Según ISO [16], esta fase tiene como propósito "asegurar y mejorar la calidad y efectividad del diseño del proceso, la implementación y los resultados".

De acuerdo con NIST [22], esta fase tiene como finalidad "mantener actualizado el conocimiento específico del riesgo en que incurren las organizaciones".

ISO 31000:2018	NIST SP 800-30	
Seguimiento y Revisión	Mantener la Evaluación	Monitorear los Factores de Riesgo
		Actualizar la Evaluación del Riesgo

Tabla 27: Seguimiento y Revisión según ISO 31000:2018 y NIST SP 800-30

4.1. MONITOREAR LOS FACTORES DE RIESGO

Según NIST [22], consiste en:

> … realizar un seguimiento continuo de los factores de riesgo que contribuyen a los cambios en el riesgo de las operaciones y los activos de la organización. La organización debe monitorear los factores de riesgo continuamente para garantizar que la información necesaria para tomar decisiones creíbles y basadas en el riesgo continúe disponible a lo largo del tiempo. El monitoreo de los factores de riesgo puede proporcionar información crítica sobre las condiciones cambiantes que podrían afectar la capacidad de la organización para llevar a cabo sus funciones.

4.2. ACTUALIZAR LA EVALUACIÓN DEL RIESGO

Según NIST [22]:

> … la evaluación del riesgo existente debe ser actualizada utilizando los resultados del monitoreo continuo de los factores de riesgo. La organización determina la frecuencia y las circunstancias en las que se actualiza la evaluación del riesgo. Si se han producido cambios significativos desde que se realizó la evaluación del riesgo, la organización puede revisar el propósito, el alcance, los supuestos y las limitaciones de la evaluación para determinar si todas las tareas en el proceso de evaluación del riesgo necesitan ser repetidas.

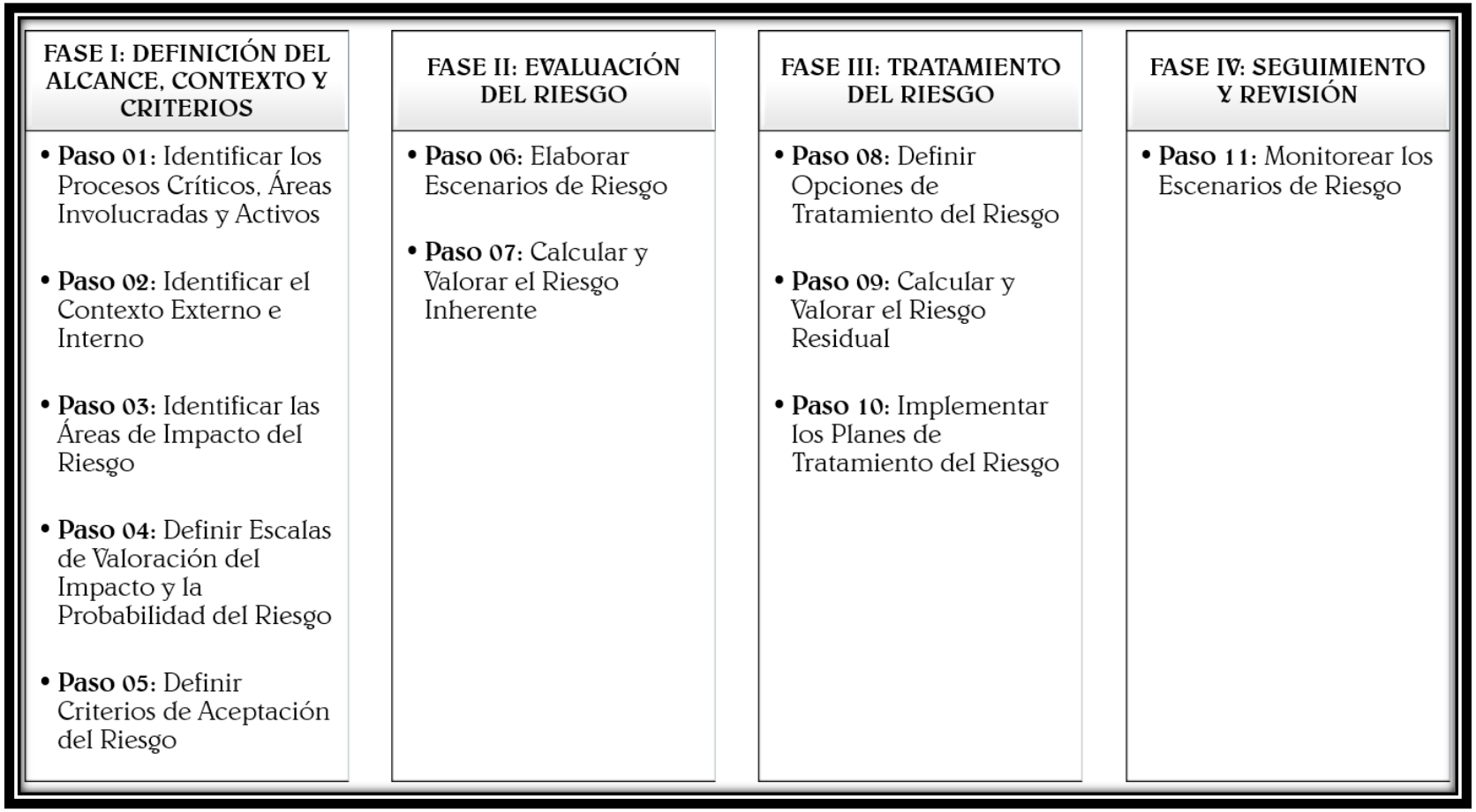
III. PROPUESTA DE SOLUCIÓN

A continuación, se muestra el proceso desarrollado como resultado del análisis de los estándares y metodologías para la gestión de riesgos, las cuales fueron adaptadas a las necesidades particulares de las empresas del sector agroindustrial, teniendo como base fundamental el estándar ISO 31000:2018.

El proceso se compone de una serie de pasos que las empresas deben seguir para implementar satisfactoriamente un proceso de gestión de riesgos de TI.

Un aspecto importante que debe ser considerado antes de comenzar con la implementación del modelo de gestión de riesgos propuesto es la composición del equipo de evaluación. Este equipo puede estar conformado por los jefes y personal de cada área quienes poseen el conocimiento de las áreas operativas, y un representante del departamento de tecnología de la información, ya que puede proporcionar la profundidad técnica que otros miembros del equipo pueden carecer. Así mismo, la participación del personal de TI es más necesaria durante el mapeo de los activos de información, el desarrollo de escenarios de riesgo y planes de mitigación.

Figura 9: Fases y Pasos Considerados en el Modelo Propuesto



Fuente: Elaboración Propia

FASE I: DEFINICIÓN DEL ALCANCE, CONTEXTO Y CRITERIOS

Su objetivo es adaptar el proceso de gestión del riesgo a la realidad particular de cada empresa, de tal manera que tanto la evaluación, así como el tratamiento del riesgo sean adecuados y efectivos, además de brindar los resultados previstos y respaldar la toma de decisiones con respecto al riesgo de TI.

Los pasos que deben ser desarrollados en esta fase son presentados a continuación:

1. PASO 01: IDENTIFICAR LOS PROCESOS CRÍTICOS, ÁREAS INVOLUCRADAS Y ACTIVOS

El propósito es garantizar que los procesos críticos, las áreas de negocio que gestionan estos procesos y los activos de la empresa sean tomados en cuenta durante el desarrollo del proceso de gestión del riesgo de TI.

1.1. Procesos Críticos

Son un conjunto de operaciones que permiten de alguna manera que la empresa siga funcionando, y que si llegan a fallar ocasionarán un impacto adverso considerable en el muy corto plazo. Estos procesos deben recibir la mayor atención, debido a que afectan directamente a la satisfacción del cliente y a la eficiencia económica de la empresa.

En el caso de las empresas del sector agroindustrial, los procesos críticos que pueden ser considerados son los siguientes:

PROCESOS CRÍTICOS EN EMPRESAS AGROINDUSTRIALES	
CÓDIGO	**PROCESO**
[PRC_001]	Recepción de Materia Prima
[PRC_002]	Procesamiento de Materia Prima
[PRC_003]	Control de Calidad
[PRC_004]	Control y Gestión de Inventarios
[PRC_005]	Compra de Materia Prima
[PRC_006]	Venta de Producto Terminado
[PRC_007]	Venta de Servicios
[PRC_008]	Gestión Logística de Suministros
[PRC_009]	Gestión de Caja y Bancos
[PRC_010]	Gestión Contable
[PRC_011]	Tecnologías de la Información

Tabla 28: Formato de Procesos Críticos en Empresas Agroindustriales

Además, es importante definir parámetros que indiquen cuanto tiempo la empresa está dispuesta a tolerar en pérdidas de datos y la caída de estos procesos críticos.

A continuación, se definen dos parámetros que permiten lograr lo antes mencionado:

- RPO (Objetivo del Punto de Recuperación): describe la antigüedad máxima de los datos para su restauración, es decir, la tolerancia que el negocio puede permitir para operar con datos de respaldo del último backup válido.
- RTO (Objetivo del Tiempo de Recuperación): define el período de tiempo permitido para la recuperación de una función o recurso de negocio a un nivel aceptable, luego de una interrupción o desastre, antes de que signifique pérdida para la empresa.

Para definir los valores del RPO y RTO de cada uno de los procesos críticos de la empresa, podemos utilizar una tabla como la que se muestra a continuación:

RPO Y RTO DE CADA PROCESO CRÍTICO			
CÓDIGO	**PROCESO**	**RPO (Horas)**	**RTO (Horas)**
[PRC_001]	Recepción de Materia Prima		
[PRC_002]	Procesamiento de Materia Prima		
[PRC_003]	Control de Calidad		
[PRC_004]	Control y Gestión de Inventarios		
[PRC_005]	Compra de Materia Prima		
[PRC_006]	Venta de Producto Terminado		
[PRC_007]	Venta de Servicios		
[PRC_008]	Gestión Logística de Suministros		
[PRC_009]	Gestión de Caja y Bancos		
[PRC_010]	Gestión Contable		
[PRC_011]	Tecnologías de la Información		

Tabla 29: Formato para Definir el RPO y RTO de cada Proceso Crítico

1.2. Áreas Involucradas

Son las áreas de negocio que gestionan los procesos críticos de la empresa y que deben ser incluidas en el alcance del proceso de gestión del riesgo de TI.

Para identificar las áreas involucradas en cada proceso crítico, podemos utilizar una tabla como la que se muestra a continuación:

ÁREAS INVOLUCRADAS EN LOS PROCESOS CRÍTICOS	
PROCESO CRÍTICO	**ÁREA**
[PRC_001] Recepción de Materia Prima	➢ ➢
[PRC_002] Procesamiento de Materia Prima	➢ ➢
[PRC_003] Control de Calidad	➢ ➢
[PRC_004] Control y Gestión de Inventarios	➢ ➢
[PRC_005] Compra de Materia Prima	➢ ➢
[PRC_006] Venta de Producto Terminado	➢ ➢
[PRC_007] Venta de Servicios	➢ ➢
[PRC_008] Gestión Logística de Suministros	➢ ➢
[PRC_009] Gestión de Caja y Bancos	➢ ➢
[PRC_010] Gestión Contable	➢ ➢
[PRC_011] Tecnologías de la Información	➢ ➢

Tabla 30: Formato para Identificar las Áreas Involucradas en los Procesos Críticos

De acuerdo a lo obtenido en la tabla anterior, podemos definir las áreas que formarán parte del alcance del proceso de gestión del riesgo, utilizando la siguiente tabla:

ÁREAS INVOLUCRADAS
1. 2. 3.

Tabla 31: Formato para Definir las Áreas de Alcance del Proceso de Gestión del Riesgo

1.3. Activos de Información

Son los elementos del sistema de información (o estrechamente relacionados con este) que intervienen en las operaciones de los procesos críticos de la empresa y que deben ser incluidos en el alcance del proceso de gestión del riesgo de TI para ser protegidos adecuadamente.

A continuación, se presenta un catálogo de activos definido por MAGERIT, que puede servir de guía para identificar los activos de información de la empresa.

CATÁLOGO DE ACTIVOS		
TIPO	**DESCRIPCIÓN**	**ACTIVOS**
[D] Datos / Información	Es un activo que puede estar almacenado en equipos o soportes de información y que puede ser transferido de un lugar a otro por los medios de transmisión de datos.	- Bases de datos. - Código fuente. - Copias de respaldo. - Datos de configuración. - Datos de control de acceso. - Ficheros.
[S] Servicios	Son funciones prestadas por el sistema que satisfacen las necesidades de los usuarios (del servicio).	- Acceso a las aplicaciones informáticas. - Acceso a la web institucional. - Correo electrónico. - Desarrollo de software. - Help Desk. - Soporte técnico.
[SW] Software (Aplicaciones Informáticas)	Estos activos gestionan, analizan y transforman los datos permitiendo la explotación de la	- Aplicaciones propias de la empresa.

CATÁLOGO DE ACTIVOS		
TIPO	**DESCRIPCIÓN**	**ACTIVOS**
	información para la prestación de los servicios.	- IDE de programación. - Paquete ofimático (Word, Excel, Power Point). - Página web institucional. - Sistema de gestión de base de datos. - Sistema operativo cliente. - Sistema operativo servidor. - Sistema SCADA (software).
[HW] Hardware (Equipos Informáticos)	Son medios físicos que almacenan, procesan o transmiten los datos, soportan la ejecución de las aplicaciones informáticas y soportan los servicios prestados a los usuarios.	- Computadoras. - Servidores. - Sistema SCADA (hardware). - Soporte de la red (switches, routers, firewalls).
[COM] Redes de Comunicaciones	Son medios de transporte que llevan datos de un sitio a otro.	- Internet. - Red local. - VPN. - Wifi.
[Media] Soportes de Información	Son dispositivos físicos que almacenan información por largos periodos de tiempo o permanentemente.	- Almacenamiento en red. - Discos externos. - Documentos impresos. - Memorias USB.

CATÁLOGO DE ACTIVOS		
TIPO	**DESCRIPCIÓN**	**ACTIVOS**
[AUX] Equipamiento Auxiliar	Son equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos.	- Equipos de climatización. - Fuentes de alimentación. - Gabinetes y racks. - Mobiliario. - UPS.
[P] Personal	Son personas relacionadas con los sistemas de información.	- Administrador de red. - Administrador de sistemas. - Desarrolladores. - Outsourcing. - Usuarios.

Tabla 32: Catálogo de Activos de Información

Finalmente, para identificar los activos que intervienen dentro de cada proceso crítico de la empresa, podemos utilizar una tabla como la que se muestra a continuación:

ACTIVOS DE INFORMACIÓN POR CADA PROCESO CRÍTICO								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
[PRC_001] Recepción de Materia Prima	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_002] Procesamiento de Materia Prima	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente. - Sistema SCADA (software).	- Computadoras. - Servidores. - Sistema SCADA (hardware). - Soporte de la red.	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_003] Control de Calidad	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático.	- Computadoras. - Servidores. - Soporte de la red.	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.

ACTIVOS DE INFORMACIÓN POR CADA PROCESO CRÍTICO								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
			- Sistema operativo cliente.					
[PRC_004] Control y Gestión de Inventarios	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_005] Compra de Materia Prima	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales. - Correo electrónico.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_006] Venta de Producto Terminado	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.

ACTIVOS DE INFORMACIÓN POR CADA PROCESO CRÍTICO								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
		- Acceso a la web de la empresa. - Correo electrónico.	- Página web institucional. - Sistema operativo cliente.					
[PRC_007] Venta de Servicios	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_008] Gestión Logística de Suministros	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales. - Correo electrónico.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.

ACTIVOS DE INFORMACIÓN POR CADA PROCESO CRÍTICO								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
[PRC_009] Gestión de Caja y Bancos	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales. - Correo electrónico.	- Aplicaciones empresariales. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_010] Gestión Contable	- Archivos informáticos. - Base de datos.	- Acceso a las aplicaciones empresariales. - Acceso a las aplicaciones contables. - Correo electrónico.	- Aplicaciones empresariales. - Aplicaciones contables. - Paquete ofimático. - Sistema operativo cliente.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - Wifi.	- Almacenamiento en red. - Discos externos. - Documentos impresos. - Memorias USB.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios.
[PRC_011] Tecnologías de la Información	- Base de datos. - Código fuente.	- Desarrollo de software. - Help Desk. - Soporte técnico.	- IDE de programación. - Paquete ofimático.	- Computadoras. - Servidores. - Soporte de la red.	- Internet. - Red local. - VPN.	- Almacenamiento en red. - Discos externos. - Documentos impresos.	- Equipos de climatización. - Fuentes de alimentación.	- Administrador de red. - Administrador de sistemas. - Desarrolladores.

ACTIVOS DE INFORMACIÓN POR CADA PROCESO CRÍTICO								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
	- Copias de respaldo. - Datos de configuración. - Datos de control de acceso.		- Sistema de gestión de base de datos. - Sistema operativo cliente. - Sistema operativo servidor.			- Memorias USB.	- Gabinetes y racks. - Mobiliario. - UPS.	- Outsourcing.

Tabla 33: Formato para Identificar los Activos de Información por cada Proceso Crítico

2. PASO 02: IDENTIFICAR EL CONTEXTO EXTERNO E INTERNO

La finalidad es identificar el entorno externo e interno en el que las empresas del sector agroindustrial llevan a cabo sus operaciones y buscan alcanzar sus objetivos.

Estos factores pueden influenciar positiva o negativamente sobre los escenarios de riesgo que afectan los procesos críticos de la empresa. Por lo tanto, el contexto externo e interno debe ser supervisado constantemente, de tal manera que el proceso de gestión del riesgo pueda responder oportunamente a los cambios que puedan presentarse.

2.1. Contexto Externo

a) **Político:** Son las entidades e instrumentos que orientan los objetivos, políticas y estrategias establecidas por los gobiernos, y que influyen en el funcionamiento, la viabilidad y la rentabilidad de las empresas del sector agroindustrial.

Entre las entidades que forman parte del entorno político de las empresas del sector agroindustrial tenemos:

- Estado Peruano.
- Ministerio de Agricultura y Riego (MINAGRI).
- Ministerio de Comercio Exterior y Turismo (MINCETUR).
- Ministerio de la Producción (PRODUCE).
- Ministerio de Economía y Finanzas (MEF).
- Gobiernos Regionales y Locales.
- Gobiernos Internacionales.

Entre las políticas que pueden influir en las empresas del sector agroindustrial tenemos:

- Política Nacional Agraria (PNA).
- Política y Estrategia Nacional de Recursos Hídricos.
- Política Nacional Forestal y de Fauna Silvestre.
- Plan Estratégico Nacional Exportador (PENX).
- Estrategia Nacional de Seguridad Alimentaria y Nutricional (ENSAN).
- Política Arancelaria.
- Normas Emitidas por los Gobiernos Regionales y Locales.
- Políticas Internacionales.
- Tratados de Libre Comercio.

b) **Legal y Regulatorio:** Conformado por un conjunto de entidades y normas que restringen y regulan las operaciones de las empresas del sector agroindustrial, pudiendo afectar positiva o negativamente los procesos críticos de la empresa.

Entre las entidades que forman parte del entorno legal y regulatorio de las empresas del sector agroindustrial tenemos:

- Dirección General de Salud Ambiental (DIGESA), encargado de formular normas sanitarias que preservan la calidad de los alimentos para prevenir la contaminación y las enfermedades transmitidas por el consumo de alimentos.
- Servicio Nacional de Sanidad Agraria (SENASA), encargado de asuntos en materia de sanidad agraria,

calidad de insumos, producción orgánica e inocuidad agroalimentaria.

- Instituto Nacional de Calidad (INACAL), encargado de certificar la calidad de los productos locales del Perú para adecuarlos a la normativa internacional y promover de esta forma su exportación.
- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), encargado de aplicar normas para proteger el mercado garantizando el respeto de los derechos de los consumidores, las normas de la honesta competencia y la propiedad intelectual.
- Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), encargado de fiscalizar el cumplimiento de las obligaciones tributarias a efecto de combatir la evasión fiscal. Además, es el responsable de la implementación, la inspección y el control del cumplimiento de la política aduanera en el territorio nacional y el tráfico internacional de mercancías.

c) **Competitivo:** Conformado por las empresas que concurren en nuestro mismo mercado para ofrecer productos o servicios similares o que buscan satisfacer las mismas necesidades de forma diferente con productos y servicios substitutos. La información acerca de los competidores permitirá a la empresa comparar y mejorar los procesos que realiza en la actualidad.

La información a recolectar acerca de la competencia podría estar conformada por:

- Sus procesos.
- Sus volúmenes de ventas.
- Los materiales o insumos que utilizan.
- La calidad de sus productos.
- Sus servicios brindados.
- Sus recursos.
- Su tecnología.

Para determinar el entorno competitivo pueden ser realizados estudios de mercado y análisis de la competencia.

d) Financiero: Corresponde a un conjunto de aspectos financieros como la inflación, la devaluación, las tasas de interés, entre otros, que pueden afectar el crecimiento económico de un país y como consecuencia afectar las decisiones comerciales, de logística, de producción, etc., de las empresas del sector agroindustrial.

Entre las entidades que forman parte del entorno financiero de las empresas del sector agroindustrial tenemos:

- Banco Central de Reserva del Perú (BCRP), encargado de preservar la estabilidad monetaria, creando condiciones necesarias para un normal desenvolvimiento de las actividades económicas, lo que contribuye a alcanzar mayores tasas de crecimiento económico sostenido.
- Banco Agropecuario (AGROBANCO), encargado de diseñar y brindar productos y servicios financieros, que complementen el desarrollo de la producción,

orientando su atención, de manera priorizada, al segmento de pequeños y medianos productores ubicados en zonas rurales.

- Otras entidades financieras.

e) **Tecnológico:** Son el conjunto de avances tecnológicos o innovaciones técnicas que surgen en el mercado y que pueden ser utilizados por la empresa para diferenciarse de sus competidores. Su repercusión se manifiesta en nuevos productos, maquinas, herramientas, materiales y servicios, que pueden contribuir al incremento de la productividad, entre otros beneficios.

No obstante, estos avances tecnológicos pueden ser utilizados para realizar ataques u otras acciones que perjudiquen a la empresa.

f) **Proveedores:** Son un conjunto de personas o empresas que nos proveen de los productos o servicios necesarios para realizar nuestra actividad empresarial.

Entre ellos tenemos a los proveedores de materia prima, de suministros, de servicio de internet, de soporte técnico, de software, entre otros.

g) **Medioambiental:** Son las características propias de la región donde las empresas del sector agroindustrial desempeñan sus actividades y que pueden afectar positiva o negativamente sus procesos. Entre los factores a tener en consideración tenemos el clima, la temperatura, la humedad, etc.

Así mismo, existen ciertos fenómenos climatológicos que deben ser tomados en cuenta:

- Sequías.
- Inundaciones.
- Fenómeno El Niño.
- Fenómeno de La Niña.
- Fenómeno de El Niño Costero.

2.2. Contexto Interno

a) **Objetivos Estratégicos:** Son las metas desarrolladas a nivel estratégico que la empresa pretende alcanzar a largo plazo para obtener mayores beneficios económicos y alcanzar una determinada posición en el mercado. Los procesos críticos de la empresa están orientados a la consecución de estos objetivos estratégicos, por lo tanto, cualquier cambio en estos objetivos puede tener un impacto en el desempeño de los mismos.

Esta información puede ser obtenida del Plan Estratégico Empresarial de la empresa.

b) **Política Interna:** Corresponde a un conjunto de principios documentados que deben ser divulgados, entendidos y acatados entre el personal de la empresa.

Esta información puede ser obtenida de los documentos de Políticas Organizacionales de la empresa.

c) **Estructura Organizacional:** Es el sistema utilizado por la empresa para definir autoridad, responsabilidad y jerarquía, de tal forma, que le permite tener una adecuada dirección y control de sus actividades.

Esta información puede ser obtenida del Organigrama Institucional de la empresa.

d) **Procesos:** Son una serie de pasos o fases que se llevan a cabo de forma secuencial dentro de la empresa para conseguir elaborar un producto o brindar un servicio.

Esta información puede ser obtenida de la Documentación de Procesos de la empresa o a través de entrevistas al personal de cada área.

e) **Infraestructura Tecnológica:** Es el conjunto de dispositivos y aplicaciones necesarios para desarrollar las actividades de la empresa. Estos elementos sirven como soporte para la administración de datos y de información en la empresa.

Esta información puede ser obtenida de los Inventarios de Activos de Información e Inventarios de Infraestructura de Tecnologías de Información.

f) **Cultura Organizacional:** Compuesta por normas, hábitos, actitudes, creencias y valores que comparten las personas o grupos de personas dentro de la empresa, y que pueden facilitar o dificultar la implementación de cualquier estrategia.

Esta información puede ser obtenida del Plan Estratégico Empresarial, Misión, Visión y Valores de cada empresa.

3. PASO 03: IDENTIFICAR LAS ÁREAS DE IMPACTO DEL RIESGO

Consiste en la identificación de los tipos de impacto que puede sufrir la empresa como resultado de la ocurrencia de un determinado escenario de riesgo. Además, estas áreas deben recibir un peso, de acuerdo al nivel de importancia o criticidad que pueden significar para la empresa.

A continuación, se presenta una tabla con las áreas de impacto propuestas para las empresas del sector agroindustrial (el peso puede ser modificado, según la empresa lo crea conveniente):

DEFINICIÓN Y PONDERACIÓN DE ÁREAS DE IMPACTO DEL RIESGO	
ÁREA DE IMPACTO	**PESO**
Operacional	30%
Reputacional	27%
Financiero	23%
Legal	20%
	Total: 100%

Tabla 34: Formato para Definir y Ponderar las Áreas de Impacto del Riesgo

4. PASO 04: DEFINIR ESCALAS DE VALORACIÓN DEL IMPACTO Y LA PROBABILIDAD DEL RIESGO

El objetivo es especificar el rango de valores que pueden tomar los factores de riesgo durante la evaluación del riesgo.

4.1. Escalas de Impacto

Representan el grado de daño que puede causar un escenario de riesgo sobre los procesos críticos de la empresa.

Las escalas son definidas para cada área de impacto identificada en el "Paso 03", tal como se muestra a continuación:

ESCALAS DE IMPACTO OPERACIONAL		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	Más del 80% de las actividades del proceso se ven afectadas.
4	Mayor	Entre el 51% y 80% de las actividades del proceso se ven afectadas.
3	Moderado	Entre el 31% y 50% de las actividades del proceso se ven afectadas.
2	Menor	Entre el 10% y 30% de las actividades del proceso se ven afectadas.
1	Insignificante	Menos del 10% de las actividades del proceso se ven afectadas.

Tabla 35: Escalas de Valoración del Impacto Operacional

ESCALAS DE IMPACTO REPUTACIONAL		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	La reputación o buena imagen de la empresa está destruida frente a los clientes, proveedores o instituciones externas.
4	Mayor	La reputación o buena imagen de la empresa se ve muy afectada frente a los clientes, proveedores o instituciones externas.
3	Moderado	La reputación o buena imagen de la empresa se ve afectada frente a los clientes, proveedores o instituciones externas.
2	Menor	La reputación o buena imagen de la empresa se ve un poco afectada frente a los clientes, proveedores o instituciones externas.
1	Insignificante	La reputación o buena imagen de la empresa no se ve afectada frente a los clientes, proveedores o instituciones externas. Sin embargo, puede verse afectada dentro de la organización.

Tabla 36: Escalas de Valoración del Impacto Reputacional

ESCALAS DE IMPACTO FINANCIERO		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	Pérdidas económicas o costos comerciales excepcionalmente elevados; que van desde S/ 1'000,000.00 a más.
4	Mayor	Pérdidas económicas o costos comerciales altamente elevados; que van desde los S/ 300,000.00 hasta S/ 999,999.99.
3	Moderado	Pérdidas económicas o costos comerciales elevados; que van desde los S/ 20,000.00 hasta S/ 299,999.99.
2	Menor	Pérdidas económicas o costos comerciales bajos; que van desde los S/ 5,000.00 hasta S/ 19,999.99.
1	Insignificante	Pérdidas económicas o costos comerciales mínimos; que van desde los S/ 0.00 hasta S/ 4,999.99.

Tabla 37: Escalas de Valoración del Impacto Financiero

ESCALAS DE IMPACTO LEGAL		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	Incumplimiento excepcionalmente grave de una ley o regulación.
4	Mayor	Incumplimiento grave de una ley o regulación.
3	Moderado	Incumplimiento de una ley o regulación.
2	Menor	Incumplimiento leve o técnico de una ley o regulación.
1	Insignificante	Incumplimiento mínimo o nulo de una ley o regulación.

Tabla 38: Escalas de Valoración del Impacto Legal

Finalmente, para calcular y valorar el impacto total que puede tener un escenario de riesgo, utilizaremos la siguiente fórmula y escala de valoración:

$$Impacto\ Total = \sum Peso\ Área\ Impacto * Valor\ Escala\ Área\ Impacto$$

ESCALAS DE IMPACTO TOTAL		
Valor	**Clasificación**	**Impacto Total**
5	Catastrófico	A partir de 3.75
4	Mayor	A partir de 3.50 y menor a 3.75
3	Moderado	A partir de 3.00 y menor a 3.5
2	Menor	A partir de 2.00 y menor a 3.00
1	Insignificante	Menor a 2.00

Tabla 39: Escalas de Valoración del Impacto Total

4.2. Escalas de Probabilidad

Representan la posibilidad de que pueda tener lugar un escenario de riesgo.

A continuación, se presentan las escalas propuestas para valorar la probabilidad:

ESCALAS DE PROBABILIDAD		
Valor	**Clasificación**	**Descripción**
5	Casi Seguro	Más de 1 vez al año.
4	Probable	Al menos 1 vez en el último año.
3	Posible	Al menos 1 vez en los últimos 2 años.
2	Poco Probable	Al menos 1 vez en los últimos 5 años.
1	Muy Raro	No se ha presentado en los últimos 5 años.

Tabla 40: Escalas de Valoración de la Probabilidad

Es importante mencionar que la descripción de las escalas puede ser modificada, según la empresa lo crea conveniente.

5. PASO 05: DEFINIR CRITERIOS DE ACEPTACIÓN DEL RIESGO

Establece los niveles de riesgo que la empresa está dispuesta a asumir para alcanzar sus objetivos.

A continuación, se presenta una propuesta de mapa de calor y criterios de aceptación del riesgo:

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Casi Seguro	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Posible	3	3	5	9	12	15
Poco Probable	2	2	4	6	8	10
Muy Raro	1	1	2	3	4	5

Tabla 41: Mapa de Calor del Riesgo

Nivel de Riesgo	Criterio de Aceptación	Descripción
[10 – 25>	Inaceptable	Riesgos que necesitan **MITIGACIÓN**: Planes de actuación **correctivos**.
[5 – 10>	Tolerable	Riesgos que necesitan **INVESTIGACIÓN**: Planes de actuación **preventivos**.
[1 – 5>	Aceptable	Riesgos que necesitan **MONITORIZACIÓN**: Planes de actuación **detectivos**.

Tabla 42: Niveles de Aceptación del Riesgo

FASE II: EVALUACIÓN DEL RIESGO

Su finalidad es identificar, analizar y valorar el riesgo dentro de la empresa. Comienza con la elaboración de escenarios de riesgo, identificando amenazas, vulnerabilidades e impactos aplicables a cada empresa. Luego, estos riesgos obtenidos son priorizados y clasificados de acuerdo a los criterios definidos anteriormente. Como resultado de este proceso obtenemos un listado de riesgos priorizados de acuerdo al nivel de riesgo y que será utilizado para informar las decisiones de respuesta al riesgo.

Los pasos que deben ser desarrollados en esta fase son presentados a continuación:

6. PASO 06: ELABORAR ESCENARIOS DE RIESGO

Consiste en establecer y describir situaciones de riesgo en la empresa, identificando amenazas, vulnerabilidades, activos y procesos críticos afectados, contextos o factores influyentes que reducen o incrementan el impacto del riesgo, así como los posibles escenarios negativos y positivos que puedan generarse. Luego, esta información será utilizada para calcular el nivel de riesgo mediante la probabilidad de ocurrencia y el impacto que puede ocasionar dicho escenario de riesgo.

6.1. Amenazas

Son los agentes, en el contexto de la gestión del riesgo, que aprovechan las vulnerabilidades para atentar contra la seguridad de un sistema de información.

El siguiente cuadro muestra algunas amenazas definidas en el anexo C de la ISO/IEC 27005:2011, que pueden afectar a las empresas agroindustriales:

CATÁLOGO DE AMENAZAS	
TIPO DE AMENAZA	**AMENAZA**
NATURALES	Fenómenos climáticos
	Inundación
	Polvo, corrosión, humedad
NO INTENCIONAL	Accidente importante
	Incendio
	Personal interno (no capacitados)
	Red energética inestable
INTENCIONAL	Clientes
	Criminales
	Entidades reguladoras
	Espionaje industrial (otras empresas)
	Ex-Empleados (renunciantes, despedidos)
	Intruso ilegal
	Outsourcing
	Personal interno (descontentos, malintencionados, negligentes, deshonestos)
	Pirata informático
	Proveedores
	Visitantes

Tabla 43: Catálogo de Amenazas

6.2. Vulnerabilidades

Son las condiciones y características propias de los sistemas de información de la empresa que la hacen susceptible a las amenazas.

El siguiente cuadro muestra algunas vulnerabilidades definidas en el anexo D de la ISO/IEC 27005:2011, que pueden presentar los sistemas de información de las empresas agroindustriales:

CATÁLOGO DE VULNERABILIDADES	
AMENAZAS	**VULNERABILIDADES**
Personal	• Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) de los contratos con el personal. • Configuración incorrecta de parámetros. • Ausencia de una política sobre limpieza de escritorio y protección de dispositivos de almacenamiento. • Especificaciones incompletas o no claras para los desarrolladores. • Ausencia de un procedimiento formal para la revisión de los derechos de acceso de los usuarios. • Ausencia de pistas de auditoria en los aplicativos informáticos. • Ausencia de protección física de la edificación (paredes, puertas y ventanas) y dispositivos de videovigilancia. • Ausencia de procedimientos de inducción al personal en el uso de los aplicativos informáticos. • Ausencia de responsabilidades en seguridad de la información en la descripción de los cargos. • Ausencia de procedimientos para evaluar correctamente las habilidades del personal de TI. • Ausencia de manuales de usuario del software. • Entrenamiento insuficiente en el uso del software. • Carencia de autenticación de usuarios en las carpetas compartidas. • Ausencia de controles para el copiado de datos y software.

CATÁLOGO DE VULNERABILIDADES	
AMENAZAS	**VULNERABILIDADES**
	• Ausencia de los procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.
Pirata Informático, Criminal Informático	• Descarga y uso no controlado de software en las estaciones de trabajo. • Deficiente configuración Routers y Firewalls. • Falta de conciencia acerca de la seguridad de la información del personal. • Carencia de pistas de auditoria para detectar accesos no autorizados. • Ausencia de procedimientos de monitoreo del tráfico de red. • Ausencia de restricciones para el acceso a internet. • Ausencia de registros en bitácoras (logs) de administrador y operario. • Habilitación de servicios innecesarios.
Entidades Reguladoras	• El número de instalaciones de un software propietario sobrepasa el número de licencias adquiridas. • Ausencia de un módulo o aplicación contable que emita comprobantes electrónicos. • Ausencia de procedimientos para introducción del software en los sistemas operativos.
Polvo, corrosión, humedad	• Susceptibilidad al polvo, corrosión y humedad. • Mantenimiento inapropiado del hardware.
Incendio	• Ubicación en área susceptible de incendios. • Carencia de un sistema de detección y alarma contra incendios. • Carencia de un sistema automático de supresión de incendios. • Carencia de extintores de fuego adecuados.

CATÁLOGO DE VULNERABILIDADES	
AMENAZAS	**VULNERABILIDADES**
Fenómenos climáticos	• Ubicación de instalaciones en áreas susceptibles de inundación. • Ausencia de protección física de la edificación. • No seguir normas internacionales para la construcción de centro de datos. • Equipos de climatización no adecuados para el uso requerido.
Red energética inestable	• Susceptibilidad de los equipos informáticos a las variaciones de voltaje. • Carencia de equipos UPS para cuando se interrumpe el suministro de energía.
Proveedores, Outsourcing	• Ausencia de acuerdos de nivel de servicio (SLAs). • Trabajo no supervisado del personal externo.

Tabla 44: Catálogo de Vulnerabilidades

6.3. Riesgo

Es la probabilidad de que una amenaza aproveche una vulnerabilidad existente, generando incidentes o situaciones de seguridad que conllevan a un daño o impacto para la empresa.

En la siguiente tabla presentamos algunos riesgos que pueden ayudarnos a definir escenarios que ocurren comúnmente en la empresa:

CATÁLOGO DE RIESGOS	
ÁMBITO	**RIESGO**
DATOS	Acceso no autorizado.
	Corrupción de datos.
	Divulgación de información.
	Manipulación no autorizada de información.
	Procesamiento ilegal de datos.
	Recepción de datos de fuentes no confiables.
	Revelación de datos sensibles.
	Robo de documentos.
	Robo de medios de información.
APLICACIONES	Abuso de privilegios.
	Aplicaciones no soportadas.
	Fallas críticas del sistema.
	Incapacidad para manejar la carga.
	Mal funcionamiento de software.
	Repudio de transacciones.
	Saturación de sistemas de información.
SEGURIDAD Y PRIVACIDAD	Ataques a sitios web.
	Ataques de malware.
	Denegación de acciones.
	Espionaje remoto.
	Insuficiencia de infraestructura de seguridad.
	Interceptación de información.
	Intrusión de software malicioso.
	Mala administración de parches.
	Phishing / Engaños intencionales.
LEGAL Y REGLAMENTARIO	Copia fraudulenta de software.
	Incumplimiento con contratos de licencias.
	Incumplimiento con reglamentos.
INFRAESTRUCTURA	Arquitectura de TI inflexible.
	Daño a los servidores.
	Destrucción de equipos o medio.
	Falla de equipos.
	Fallas en aire acondicionado.
	Fallas en equipos de telecomunicación.

CATÁLOGO DE RIESGOS	
ÁMBITO	**RIESGO**
	Hardware deficiente.
	Robo de equipos.
	Tecnología obsoleta.
ENTORNO FÍSICO	Desastres naturales.
	Fallas de energía eléctrica.
	Huelgas.
	Incendio.
	Infiltración de agua de lluvia.
	Sanciones ambientales.
PERSONAL	Acciones de empleados descontentos contra la empresa.
	Desconocimiento del usuario.
	Falta de conocimiento del negocio.
	Habilidades inadecuadas.
	Incapacidad para reclutar personal de TI.
	Negligencia del usuario.
	Pérdida de recursos clave de TI.
PROVEEDORES Y OUTSOURCING	Fuga de datos.
	Nivel de servicio bajo.
	Soporte inadecuado.

Tabla 45: Catálogo de Riesgos

6.4. Escenario de Riesgo

Es la representación y análisis de la interacción de los factores de riesgo (amenaza, vulnerabilidad y la influencia del contexto) determinando las posibles consecuencias negativas o positivas que podrían generarse.

A continuación, se presenta un formato que puede ser utilizado para definir los escenarios de riesgo de la empresa:

FORMATO PARA DEFINIR ESCENARIOS DE RIESGO	
Código	Identificador del escenario.
Riesgo	Incidente o situación de seguridad.
Tipo de amenaza	Clasificación de la amenaza (Natural, No Intencional, Intencional).
Amenaza	Agente que puede explotar las vulnerabilidades.
Vulnerabilidad	Condición o característica que puede ser aprovechada por una amenaza.
Escenario negativo	Resultado negativo o no deseado, producto de la materialización u ocurrencia de un riesgo.
Activos afectados	Elementos del sistema de información que pueden verse afectados por la materialización del riesgo.
Procesos afectados	Operaciones críticas de la empresa que pueden verse afectadas por la materialización del riesgo.
Contexto influyente	Factores internos o externos que pueden reducir o incrementar los efectos del riesgo.
Duración	Período de tiempo que permanece el efecto del riesgo.
Escenario positivo	Resultado positivo u oportunidad generada a partir de realizar correctamente la gestión del riesgo.

Tabla 46: Formato para Definir Escenarios de Riesgo

7. PASO 07: CALCULAR Y VALORAR EL RIESGO INHERENTE

Consiste en estimar el nivel de riesgo de cada escenario identificado, a través de la combinación de la probabilidad de que una amenaza explote una vulnerabilidad y el impacto adverso resultante, todo esto antes de aplicar salvaguardas. Posteriormente, se realizará una comparación entre los resultados obtenidos con los criterios de aceptación del riesgo establecidos por la empresa.

Para calcular y valorar el nivel de riesgo inherente en la empresa podemos utilizar la siguiente tabla:

N°	Escenario de Riesgo		Impacto						Probabilidad (P)	Nivel de Riesgo (I * P)	Criterio de Aceptación
	Código	Riesgo	Impacto Operacional (0.30)	Impacto Reputacional (0.27)	Impacto Financiero (0.23)	Impacto Legal (0.20)	Impacto Total	Impacto (I)			
1	[ESC_RIE_001]	Riesgo 001	3	4	4	3	3.50	4	3	12	Inaceptable
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											

Tabla 47: Formato para Calcular y Valorar el Nivel de Riesgo Inherente

FASE III: TRATAMIENTO DEL RIESGO

Su objetivo es seleccionar e implementar opciones para afrontar aquellos escenarios de riesgo que han sido identificados y valorados, obteniendo como resultado un nivel de riesgo residual, es decir, un nivel de riesgo resultante que sea aceptado por la empresa luego de implementar dichas opciones de tratamiento.

Los pasos que deben ser desarrollados en esta fase son presentados a continuación:

8. PASO 08: DEFINIR OPCIONES DE TRATAMIENTO DEL RIESGO

El propósito es identificar las opciones más convenientes para hacer frente a los escenarios de riesgo definidos anteriormente, equilibrando los beneficios esperados contra el esfuerzo, las desventajas o el costo de implementar estas opciones.

Las opciones de tratamiento del riesgo que pueden ser consideradas por la empresa son las siguientes:

8.1. Aceptar el Riesgo

Consiste en retener el nivel de riesgo actual, puesto que cumple con los criterios de aceptación definidos o por decisión del gobierno de la empresa, por lo tanto, no hay necesidad de implementar algún control adicional. Este nivel de riesgo debe ser conocido y aceptado formalmente por la alta dirección.

8.2. Mitigar el Riesgo

El objetivo es reducir el impacto causado por una amenaza y/o reducir la probabilidad de que una amenaza se materialice, de tal forma que, el nivel de riesgo residual pueda

cumplir con los criterios de aceptación definidos por la empresa. Para eso, se deben introducir, alterar o eliminar ciertos controles o salvaguardas.

Es importante identificar los controles o salvaguardas existentes con la finalidad de evitar esfuerzos o costos innecesarios generados por la duplicación de los mismos. Las salvaguardas existentes deben ser verificadas para garantizar que continúen siendo adecuadas para el entorno en el que se encuentran, puesto que, su incorrecto funcionamiento puede generar vulnerabilidades.

MAGERIT proporciona algunos controles o salvaguardas que pueden ser considerados:

CATÁLOGO DE CONTROLES O SALVAGUARDAS	
TIPO	**SALVAGUARDA**
Generales	- Gestión de incidencias. - Gestión de privilegios. - Organización de la seguridad: roles, comités. - Política corporativa de seguridad de la información. - Procedimientos de continuidad de operaciones.
Protección de los datos / información	- Cifrado. - Cláusulas de confidencialidad en los contratos de trabajo. - Control de acceso. - Copias de seguridad. - Política de escritorio limpio. - Política sobre el uso de dispositivos externos. - Registro de incidencias. - Soluciones Data Loss Prevention (DLP).

CATÁLOGO DE CONTROLES O SALVAGUARDAS	
TIPO	**SALVAGUARDA**
Protección de las aplicaciones (software)	- Actualizaciones del sistema operativo y aplicaciones. - Antivirus. - Gestión adecuada de accesos y perfiles de usuario. - Gestión de cambios y configuración. - Gestión de incidencias. - Metodologías para desarrollo de software seguro. - Procedimientos para la implantación de aplicaciones. - Soluciones Data Loss Prevention (DLP). - Tablas y campos de auditoria en la base de datos.
Protección de los equipos (hardware)	- Control de equipos que salen de las instalaciones. - Estabilizadores de voltaje. - Inventario de equipos. - Mantenimiento de equipos. - Medidas de protección física. - UPS.
Protección de las comunicaciones	- Adquisición y mantenimiento de dispositivos de red. - Configuración de Firewalls. - Configuración de Routers. - Monitorear las IPs que están accediendo al servidor. - Monitorización de uso de la red. - Planificación de capacidad. - Segregación de redes.
Protección de las instalaciones	- Acondicionar los ambientes para evitar la infiltración. - Barreras físicas (paredes, puertas, ventanas, etc.). - Cámaras de seguridad.

CATÁLOGO DE CONTROLES O SALVAGUARDAS	
TIPO	**SALVAGUARDA**
	- Control de acceso: entrada y salida de personas, equipos, soportes de información, etc. - Extintores. - Protección del cableado (canaletas). - Protección frente a accidentes industriales como incendio, polvo, etc. - Protección frente a accidentes naturales como inundaciones, fuertes lluvias, etc. - Reubicación del centro de datos.
Relativas al personal	- Capacitaciones continuas. - Concientización en cultura de seguridad de la información. - Condiciones contractuales: responsabilidad en seguridad. - Desarrollo y actualización periódica de los manuales de usuario. - Proceso de inducción adecuado. - Selección de personal.
Relativas a los proveedores	- Acuerdo de confidencialidad, acuerdo de no divulgación (NDA). - Acuerdo de Nivel de Servicio (SLA). - Contratar servicios de proveedor de Internet o hosting web especializados en protección DDoS. - Identificación y calificación del personal encargado. - Procedimientos de resolución de incidencias.
Relativas a las regulaciones	- Adquisición de licencias de software. - Contratar un Operador de Servicios Electrónicos (OSE). - Emisión de comprobantes electrónicos en el sistema. - Gestión de software instalado. - Utilizar software libre.

Tabla 48: Catálogo de Controles o Salvaguardas

8.3. Compartir el Riesgo

Consiste en dividir las responsabilidades o consecuencias de ciertos riesgos con terceros. Los riesgos cualitativos (técnicos y legales) pueden ser compartidos a través de la externalización de componentes, mientras que los riesgos cuantitativos (económicos) pueden ser compartidos a través de la contratación de seguros.

8.4. Evitar el Riesgo

El objetivo es modificar las condiciones bajo las cuales se viene operando y que traen como consecuencia riesgos o costos de tratamiento del riesgo demasiado altos. Esto puede implicar, en algunos casos dejar de realizar las actividades o prescindir de aquellos componentes que generan el riesgo, siempre y cuando esto no permita dejar de llevar a cabo la misión de la empresa.

9. PASO 09: CALCULAR Y VALORAR EL RIESGO RESIDUAL

Consiste en estimar el nivel de riesgo de cada escenario identificado, después de aplicar cualquiera de las opciones de tratamiento definidas en el "Paso 08". Posteriormente, se realizará una comparación entre los resultados obtenidos con los criterios de aceptación del riesgo establecidos por la empresa.

A continuación, se presenta un formato que puede ser utilizado para seleccionar las opciones de tratamiento por cada escenario de riesgo identificado:

FORMATO PARA SELECCIONAR OPCIONES DE TRATAMIENTO						
ESCENARIO DE RIESGO						
Código						
Riesgo						
Tipo de Amenaza						
Amenaza						
Vulnerabilidad						
Escenario Negativo						
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel de Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)						
Reputacional (0.27)						
Financiero (0.23)						
Legal (0.20)						
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes		**Salvaguardas a Implementar**				
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel de Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)						
Reputacional (0.27)						
Financiero (0.23)						
Legal (0.20)						

Tabla 49: Formato para Seleccionar Opciones de Tratamiento del Riesgo

N°	Escenario de Riesgo		Riesgo Inherente				Tratamiento		Riesgo Residual			
	Código	Riesgo	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación	Opción	Salvaguardas	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación
1	[ESC_RIE_001]	Riesgo 001	4	3	12	Inaceptable	Mitigar	- Salvaguarda 1, Salvaguarda 2	4	1	4	Aceptable
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												

Tabla 50: Formato Resumen de Selección de Opciones de Tratamiento

10. PASO 10: IMPLEMENTAR LOS PLANES DE TRATAMIENTO DEL RIESGO

Consiste en formular una serie de proyectos que pondrán en marcha aquellas opciones de tratamiento que han sido seleccionadas por la empresa para abordar los escenarios de riesgo existentes.

Para realizar la formulación de los proyectos, la empresa puede hacer uso de un formato como el que se muestra a continuación:

FORMATO PARA LA PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
Identificador del Proyecto.	
2) NOMBRE DEL PROYECTO	
Descripción del Proyecto.	
3) RESPONSABLE	
Nombre	**Cargo**
Encargado de implementar el proyecto.	Puesto de la persona encargada del proyecto.
4) FECHA	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
6) JUSTIFICACIÓN	
Fundamentar la importancia del proyecto.	
7) ALTERNATIVAS	
Otras opciones que pueden ser consideradas en lugar del proyecto.	
8) ÁREAS BENEFICIARIAS	
Áreas de la empresa que serán beneficiadas con el proyecto.	
9) CONCLUSIONES	
Consecuencias o resultados esperados del proyecto.	

Tabla 51: Formato para la Presentación de Proyectos para el Tratamiento del Riesgo

FASE IV: SEGUIMIENTO Y REVISIÓN

Su objetivo es asegurar y mejorar, la calidad y efectividad del proceso de gestión del riesgo, así como, mantener actualizado el conocimiento acerca de los escenarios de riesgo existentes en la empresa.

El paso que debe ser desarrollado en esta fase se presenta a continuación:

11. PASO 11: MONITOREAR LOS ESCENARIOS DE RIESGO

Consiste en definir un conjunto de métricas que permitan supervisar cada escenario de riesgo, asegurando que la información obtenida en el análisis, los controles implementados y los niveles de riesgo continúen siendo apropiados.

Además, debemos revisar los cambios en los factores externos e internos que pueden influir positiva o negativamente en el estado del riesgo, de tal modo que, pueda ser necesario realizar modificaciones a la evaluación y tratamiento del riesgo.

COBIT 5 proporciona un conjunto de métricas que podemos utilizar para monitorear los escenarios de riesgo. Cabe mencionar, que la empresa puede agregar las métricas que crea conveniente.

CATÁLOGO DE MÉTRICAS PARA LOS ESCENARIOS DE RIESGO	
ÁMBITO	**MÉTRICA**
Cumplimiento de Leyes y Regulaciones Externas	• Coste de incumplimientos de TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación. • Número de incumplimientos de TI reportados a la Alta Dirección o causantes de comentarios o vergüenza pública. • Número de incumplimientos relacionados con proveedores de servicios de TI.
Entrega de Servicios de TI	• Número de interrupciones de negocio debido a incidentes de servicios de TI. • Porcentaje de partes interesadas en el negocio satisfechas de que los servicios de TI cumplan con los niveles de servicio acordados. • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios de TI.
Uso adecuado de aplicaciones y soluciones tecnológicas	• Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios de TI. • Nivel de entendimiento de los usuarios de negocio sobre cómo las soluciones tecnológicas apoyan sus procesos. • Nivel de satisfacción de los usuarios de negocio con la formación y los manuales de usuario.
Agilidad de las TI	• Nivel de satisfacción de la Alta Dirección con la capacidad de respuesta de TI a nuevos requerimientos. • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas.
Seguridad de la información, infraestructuras de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública. • Número de servicios de TI sin requerimientos de seguridad destacables.

CATÁLOGO DE MÉTRICAS PARA LOS ESCENARIOS DE RIESGO	
ÁMBITO	**MÉTRICA**
	• Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías.
Soporte de procesos de negocio integrando aplicaciones y tecnología	• Número de incidentes del procesamiento de negocio causados por errores de integración de la tecnología. • Número de cambios en los procesos de negocio que tienen que ser retrasados o revisados debido a problemas de integración de la tecnología. • Número de programas de negocio facilitados por TI retrasados o incurriendo en costes adicionales debido a problemas de integración de la tecnología. • Número de aplicaciones o infraestructuras críticas operando aisladamente y no integradas.
Disponibilidad de información	• Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión. • Número de incidentes de procesos de negocio causados por la indisponibilidad de la información. • Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave.
Cumplimiento de las políticas internas	• Número de incidentes relacionados con el incumplimiento de políticas. • Porcentaje de usuarios que entienden las políticas. • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas. • Frecuencia de revisión y actualización de políticas.
Personal	• Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles.

CATÁLOGO DE MÉTRICAS PARA LOS ESCENARIOS DE RIESGO	
ÁMBITO	**MÉTRICA**
	• Porcentaje de personal satisfecho con sus roles en TI. • Número de horas de aprendizaje / formación por miembro del personal.

Tabla 52: Catálogo de Métricas para los Escenarios de Riesgo

La empresa puede utilizar el siguiente formato para definir las métricas que permitirán monitorear los escenarios de riesgo analizados en los pasos previos:

FORMATO PARA MONITOREAR LOS ESCENARIOS DE RIESGO		
ESCENARIO DE RIESGO		
Código	Identificador del escenario.	
Riesgo	Incidente o situación de seguridad.	
Tipo de Amenaza	Clasificación de la amenaza (Natural, No Intencional, Intencional).	
Amenaza	Agente externo o interno que puede explotar las vulnerabilidades.	
Vulnerabilidad	Condición o característica que puede ser aprovechada por una amenaza.	
Escenario Negativo	Resultado negativo o no deseado, producto de la materialización u ocurrencia de un riesgo.	
SALVAGUARDAS IMPLEMENTADAS		
Controles implementados para mitigar el nivel de riesgo.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Factores internos o externos que pueden reducir o incrementar los efectos del riesgo.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
Son aquellos datos expresados numéricamente que sirven para analizar el estado del riesgo.	Son los diversos tipos de instrumentos que contienen datos útiles para la métrica definida.	Valor de control referencial para la métrica definida.

Tabla 53: Formato para Monitorear los Escenarios de Riesgo

IV. DISCUSIÓN

Según el objetivo general planteado en el presente proyecto tesis de contribuir en la mejora de la seguridad de los activos de información en las empresas del sector agroindustrial de la región Lambayeque, se desarrolló el modelo basado en metodologías de gestión de riesgos de TI.

La validación del modelo se realizó a través del juicio de expertos, para lo cual 4 profesionales expertos validaron la estructura y el contenido del modelo propuesto en el presente proyecto de tesis, obteniendo la aceptación del mismo (Ver Anexo N° 06).

Para evaluar la confiabilidad del modelo propuesto, en cuanto a su estructura o contenido, y determinar el grado de concordancia entre los profesionales expertos, se utilizaron dos instrumentos:

4.1. Alpha de Cronbach

Este coeficiente se utilizó para medir el nivel de confiabilidad del modelo.

Ruiz [24], proporciona una manera práctica de interpretar el coeficiente de confiabilidad guiada por la escala mostrada en el siguiente cuadro:

RANGOS	MAGNITUD
0.81 a 1.00	Muy Alta
0.61 a 0.80	Alta
0.41 a 0.60	Moderada
0.21 a 0.40	Baja
0.01 a 0.20	Muy Baja

Tabla 54: Escala del Coeficiente de Confiabilidad

Los resultados del juicio de expertos fueron procesados aplicando Alpha de Cronbach, obteniendo un nivel de confiabilidad del **81.0%**, lo que significa, que la confiabilidad del modelo propuesto es **Muy Alta**.

ESTADÍSTICAS DE CONFIABILIDAD	
Alfa de Cronbach	**N de elementos**
0.810	21

Tabla 55: Resultados del Procesamiento de Alpha de Cronbach

4.2. Concordancia de Kendall

Este coeficiente se utilizó para determinar el grado de concordancia de las evaluaciones realizadas por los expertos.

Los valores del coeficiente de concordancia W de Kendall pueden variar de 0 a 1. Mientras mayor sea el valor del coeficiente de Kendall, más fuerte será la concordancia.

Escobar y Cuervo [25], proporcionan un cuadro resumen del estadístico para realizar el análisis de los datos obtenidos:

HIPÓTESIS	RECHAZO DE H_0 E INTERPRETACIÓN
H_0: Los rangos son independientes, no concuerdan. H_1: Hay concordancia significativa entre los rangos.	Se rechaza H_0 cuando el valor observado excede al valor crítico (con un α de 0.05). El SPSS indica el nivel de significancia, y cuando es inferior al 0.05, se rechaza la H_0 y se concluye que hay concordancia significativa entre los rangos asignados por los jueces. Además, se interpreta la fuerza de la concordancia, que aumenta cuando W se acerca a 1.

Tabla 56: Hipótesis e Interpretación del Coeficiente de Concordancia de Kendall

De acuerdo a los resultados obtenidos del juicio de expertos se acepta la hipótesis alterna, es decir, que existe concordancia entre las opiniones de los expertos y que este valor es significativo ($p = 0.004 < 0.05$).

ESTADÍSTICOS DE PRUEBA	
N	22
W de Kendall	0.199
Chi-Cuadrado	13.135
gl (grados de libertad)	3
Sig (valor de p)	0.004

Tabla 57: Resultados del Procesamiento de Concordancia de Kendall

Finalmente, según los resultados obtenidos en los métodos estadísticos aplicados a la evaluación del modelo, se puede afirmar que el nivel de confiabilidad del modelo propuesto es muy alto y que existe concordancia significativa entre las opiniones de los 4 expertos.

CONCLUSIONES

1. Se realizó el análisis y armonización de conceptos, estándares y metodologías de gestión de riesgos de TI, de tal forma, que se adecuen a las empresas del sector agroindustrial de la región. Este tipo de propuesta de armonización ha sido realizada con anterioridad para diversos tipos de empresas de Lambayeque, sin embargo, no se encontró antecedente alguno de una propuesta similar aplicada a las empresas del sector agroindustrial.

2. Se consiguió desarrollar el modelo propuesto de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región. Comienza con la identificación de procesos críticos y activos de información que intervienen en dichos procesos. También, se realiza la elaboración de escenarios de riesgo que pueden afectar a los procesos y activos. Luego, se proponen opciones de tratamiento para mitigar los riesgos que no son aceptables para la empresa. Finalmente, se definen métricas que permitan monitorizar los escenarios de riesgo.

3. Se validó la implementación del modelo propuesto de gestión de riesgos de TI en una empresa del sector agroindustrial de la región. Como resultado de la implementación del modelo, fueron identificados 20 escenarios de riesgo, de los cuales 13 eran clasificados como Inaceptables y 7 como Tolerables. Para los escenarios cuyos niveles de riesgo no eran aceptables para la empresa, se propusieron 8 proyectos que permitirían disminuir el nivel de riesgo existente.

4. Se validó el modelo propuesto de gestión de riesgos de TI a través del juicio de expertos, quienes determinaron su utilidad para las empresas del sector agroindustrial de la región. El nivel de confiabilidad se comprobó utilizando el coeficiente Alpha de Cronbach, cuyo valor fue de 0.810, lo que significa, que la confiabilidad del modelo es muy alta. Por otro lado, el nivel de concordancia de las evaluaciones realizadas por los expertos se comprobó mediante el coeficiente de concordancia de Kendall, obteniendo un nivel de significancia inferior al 0.05, lo que quiere decir, que existe concordancia significativa entre las opiniones de los expertos.

REFERENCIAS BIBLIOGRÁFICAS

[1] ISACA, *COBIT 5: Procesos Catalizadores*. EE.UU., 2012.

[2] Consejo Superior de Administración Electrónica, *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid, 2012.

[3] A. Ramírez and Z. Ortiz, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," *Ingeniería*, vol. 16, no. 2, pp. 56–66, 2011.

[4] ESET, "ESET Security Report: Latinoamérica 2018," Buenos Aires, 2018.

[5] T. Harford, "High-frequency trading and the $440m mistake," *BBC News*, 2012. [Online]. Disponible: https://bbc.in/2ODWSrj.

[6] C. Baraniuk, "Thousands of Delta passengers delayed by computer bug," *BBC News*, 2016. [Online]. Disponible: https://bbc.in/2Mfi7mx.

[7] K. Peachey, "Tesco Bank attack was unprecedented, says regulator," *BBC News*, 2016. [Online]. Disponible: https://bbc.in/2nBdTae.

[8] EL TIEMPO, "Multa de $ 840 millones a Bancolombia por fallas técnicas," *EL TIEMPO*, 2017. [Online]. Disponible: https://bit.ly/2nDP7WP.

[9] RPP Noticias, "Indecopi multó a Interbank con S/ 76,950 por caída de sistema," *RPP Noticias*, 2017. [Online]. Disponible: https://bit.ly/2w5e9Cf.

[10] D. E. Moncayo, "Modelo de evaluación de Gestión de Riesgos en activos de TIC's para una empresa del Sector Automotriz.," Escuela Politécnica Nacional, 2014.

[11] J. J. Martínez, "Controles de seguridad para reducir la cantidad de incidencias de seguridad de la información del año 2012 en el Servicio de Administración Tributaria de Huancayo," Universidad Nacional del Centro del Perú, 2014.

[12] S. Amador, "Gestión del riesgo con base en ISO27005 adaptando OCTAVE-S," Universidad Internacional de la Rioja, 2014.

[13] M. F. Molina, "Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral," Universidad Politécnica de Madrid, 2015.

[14] F. M. Arévalo, I. P. Cedillo, and S. A. Moscoso, "Metodología Ágil para la Gestión de Riesgos Informáticos," *Rev. Kill. Técnica*, vol. 1, no. 2, pp. 31–42, 2017.

[15] ISACA, *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa*. EE.UU., 2012.

[16] International Organization for Standardization, *Risk management -*

Guidelines, ISO 31000:2018. 2018.

[17] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. 2007.

[18] National Institute of Standards and Technology, "Managing Information Security Risk, NIST SP 800-39," Gaithersburg, 2011.

[19] Parlamento Europeo, *Reglamento (CE) 460/2004, de 10 de marzo 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información*. 2004.

[20] Instituto Nacional de Ciberseguridad de España, "Gestión de Riesgos: Una guía de aproximación para el empresario," 2015.

[21] International Organization for Standardization, *Information technology - Security techniques - Information security risk management, ISO/IEC 27005:2011*. 2011.

[22] National Institute of Standards and Technology, "Guide for conducting risk assessments, NIST SP 800-30," 2012.

[23] Instituto Nacional de Estadística e Informática, "Lambayeque Indicadores de Potencialidades 2011 - 2016," 2017.

[24] C. Ruiz, "Confiabilidad," *Programa Interinstitucional Dr. en Educ.*, p. 12, 2019.

[25] J. Escobar and Á. Cuervo, "Validez de contenido y juicio de expertos: una aproximación a su utilización," *Univ. El Bosque, Colomb. Inst. Univ. Iberoam. Colomb.*, 2008.

ANEXOS

ANEXO 1: CUESTIONARIO PARA EL ENCARGADO DEL ÁREA DE TI

EMPRESA: .....

CARGO: .....

NOTA: Se está realizando un estudio acerca de la **gestión de riegos** de los activos de TI, con la finalidad de identificar el estado actual del riesgo y como se viene realizando la gestión de los mismos en el interior de la organización. Para lograrlo, necesitamos que nos ayude contestando con sinceridad algunas preguntas sencillas. Esta información tiene carácter **anónimo**.

INDICACIONES: MARQUE CON UNA X LA RESPUESTA SELECCIONADA POR USTED

N°	PREGUNTA	SI	PARCIAL	NO
1	¿Se ha establecido un método para identificar, clasificar y analizar datos relacionados con los riesgos de TI?			
2	¿Se ha realizado un análisis de datos históricos de riesgos de TI en empresas similares de la industria?			
3	¿Se ha determinado las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo?			
4	¿Se ha establecido el alcance del análisis de riesgos?			
5	¿Se ha construido escenarios de riesgo de TI?			
6	¿Se ha realizado una comparación del riesgo residual (riesgo después de aplicar controles) con la tolerancia al riesgo definida por la organización?			
7	¿Se ha realizado un análisis coste-beneficio de las opciones de respuesta al riesgo potencial?			
8	¿Se ha identificado y establecido controles clave de mitigación para estos riesgos?			
9	¿Se ha validado los resultados del análisis de riesgos antes de usarlos para la toma de decisiones?			
10	¿Se ha determinado que servicios de TI y recursos de infraestructura de TI son esenciales para sostener la operación de los procesos de negocio?			
11	¿Se informa de los resultados del análisis de riesgos a todas las partes interesadas?			
12	¿Se revisan los resultados de evaluaciones externas y auditorías internas para determinar la necesidad de análisis de riesgos adicionales?			

13	¿Se mantiene un inventario de actividades de control que estén en marcha para gestionar el riesgo?			
14	¿Se ha definido proyectos para reducir el efecto del riesgo actual?			
15	¿Se ha documentado planes que especifiquen los pasos a seguir cuando un evento de riesgo pueda causar un incidente significativo?			

NOMBRE: .....

DNI: .....

HA SIDO VALIDADA CON RESPECTO A COBIT 5.

ANEXO 2: RESULTADOS DEL CUESTIONARIO PARA EL ENCARGADO DEL ÁREA DE TI

N°	PREGUNTA	EMPRESA 01	EMPRESA 02	EMPRESA 03	EMPRESA 04
1	¿Se ha establecido un método para identificar, clasificar y analizar datos relacionados con los riesgos de TI?	Parcial	No	No	Parcial
2	¿Se ha realizado un análisis de datos históricos de riesgos de TI en empresas similares de la industria?	No	Parcial	No	No
3	¿Se ha determinado las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo?	Si	Parcial	Parcial	Parcial
4	¿Se ha establecido el alcance del análisis de riesgos?	No	No	No	Si
5	¿Se ha construido escenarios de riesgo de TI?	Si	No	No	Parcial
6	¿Se ha realizado una comparación del riesgo residual (riesgo después de aplicar controles) con la tolerancia al riesgo definida por la organización?	No	Parcial	No	Parcial
7	¿Se ha realizado un análisis coste-beneficio de las opciones de respuesta al riesgo potencial?	No	No	Parcial	No
8	¿Se ha identificado y establecido controles clave de mitigación para estos riesgos?	Si	Parcial	Parcial	Parcial
9	¿Se ha validado los resultados del análisis de riesgos antes de usarlos para la toma de decisiones?	No	No	No	Si

10	¿Se ha determinado que servicios de TI y recursos de infraestructura de TI son esenciales para sostener la operación de los procesos de negocio?	Si	Si	Si	Parcial
11	¿Se informa de los resultados del análisis de riesgos a todas las partes interesadas?	No	No	No	Parcial
12	¿Se revisan los resultados de evaluaciones externas y auditorías internas para determinar la necesidad de análisis de riesgos adicionales?	No	Parcial	No	Parcial
13	¿Se mantiene un inventario de actividades de control que estén en marcha para gestionar el riesgo?	Si	No	No	Si
14	¿Se ha definido proyectos para reducir el efecto del riesgo actual?	Parcial	No	Parcial	Parcial
15	¿Se ha documentado planes que especifiquen los pasos a seguir cuando un evento de riesgo pueda causar un incidente significativo?	No	No	Parcial	No

ANEXO 3: GRÁFICOS DE LOS RESULTADOS DEL CUESTIONARIO

Gráfico 1: ¿Se ha establecido un método para identificar, clasificar y analizar datos relacionados con los riesgos de TI?

Gráfico 2: ¿Se ha realizado un análisis de datos históricos de riesgos de TI en empresas similares de la industria?

Gráfico 3: ¿Se ha determinado las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo?

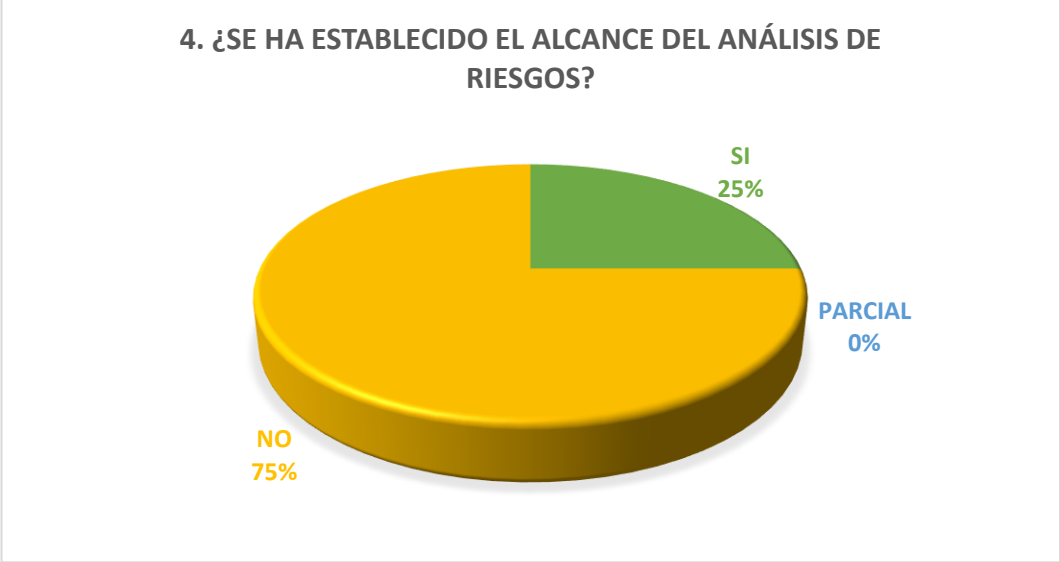


Gráfico 4: ¿Se ha establecido el alcance del análisis de riesgos?

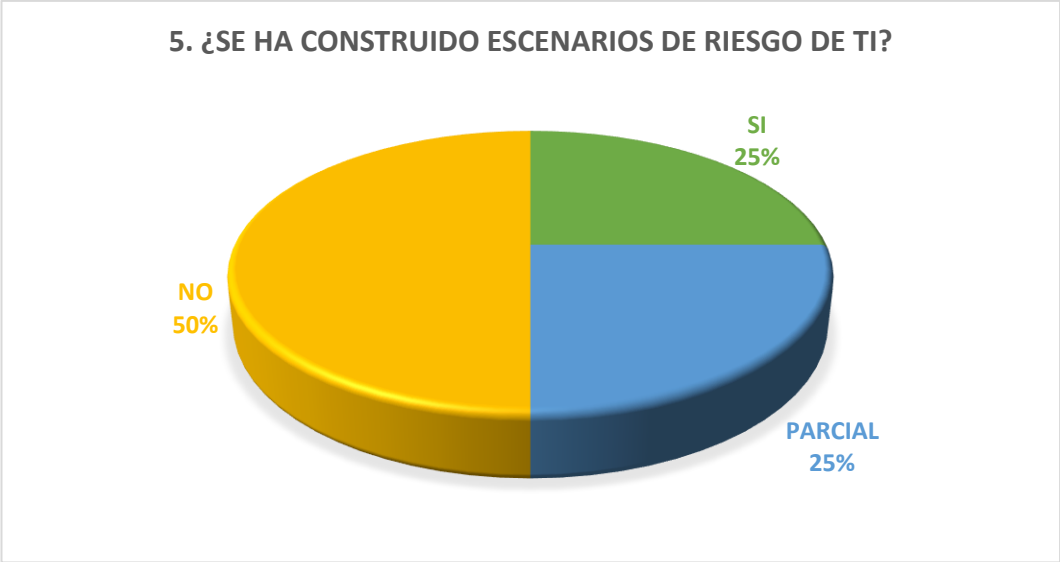


Gráfico 5: ¿Se ha construido escenarios de riesgo de TI?

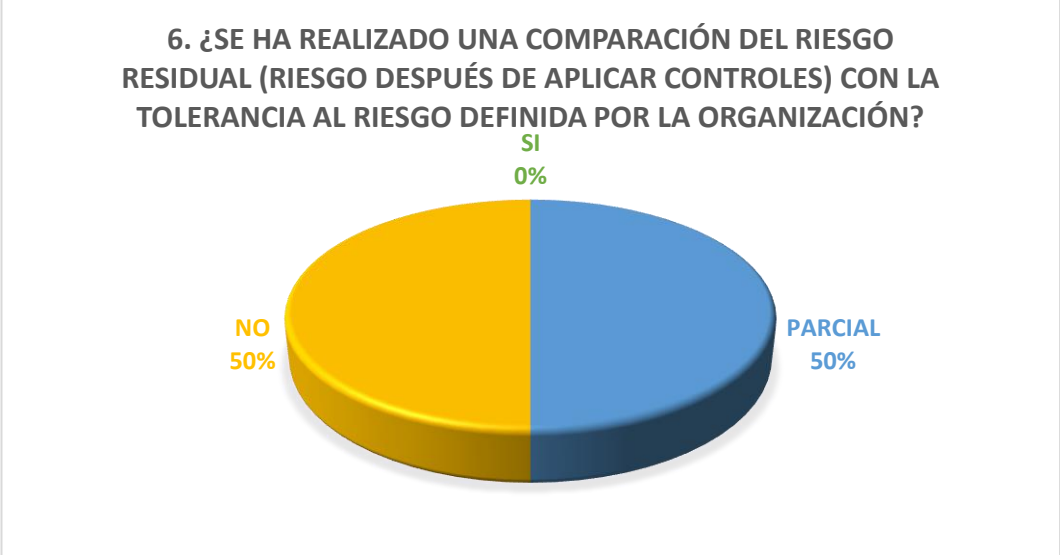


Gráfico 6: ¿Se ha realizado una comparación del riesgo residual (riesgo después de aplicar controles) con la tolerancia al riesgo definida por la organización?

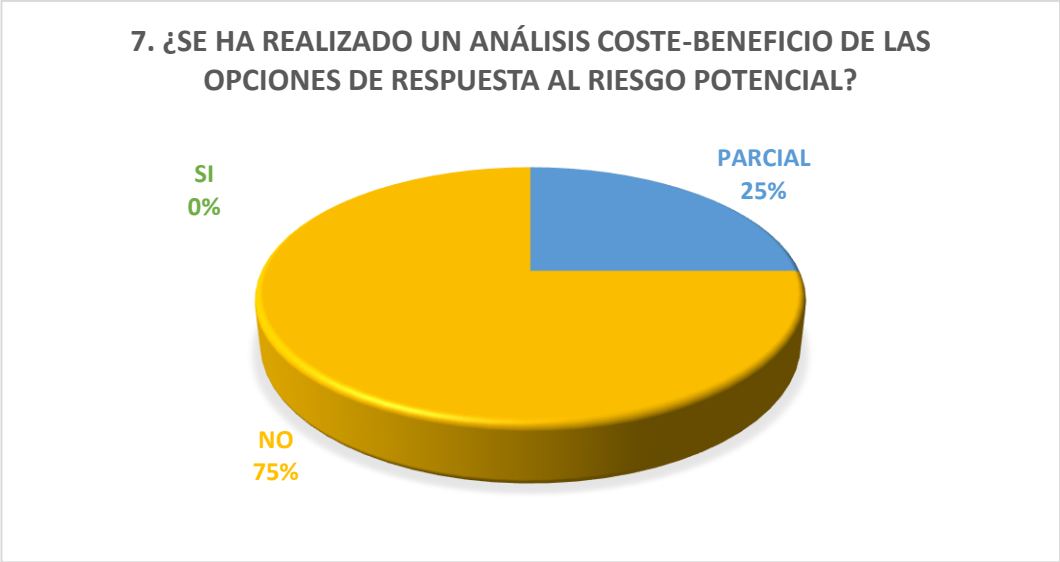


Gráfico 7: ¿Se ha realizado un análisis coste-beneficio de las opciones de respuesta al riesgo potencial?

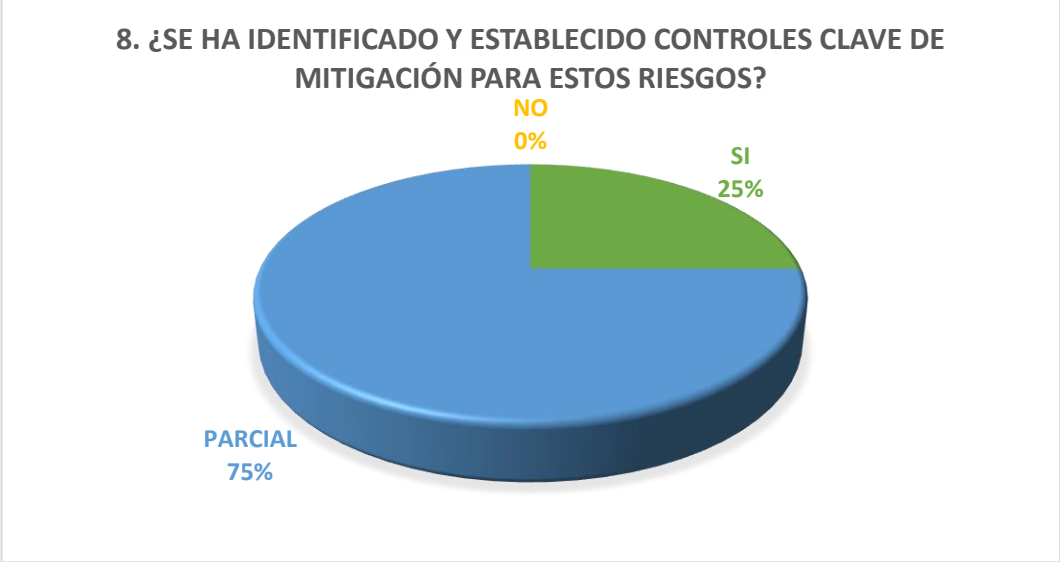


Gráfico 8: ¿Se ha identificado y establecido controles clave de mitigación para estos riesgos?

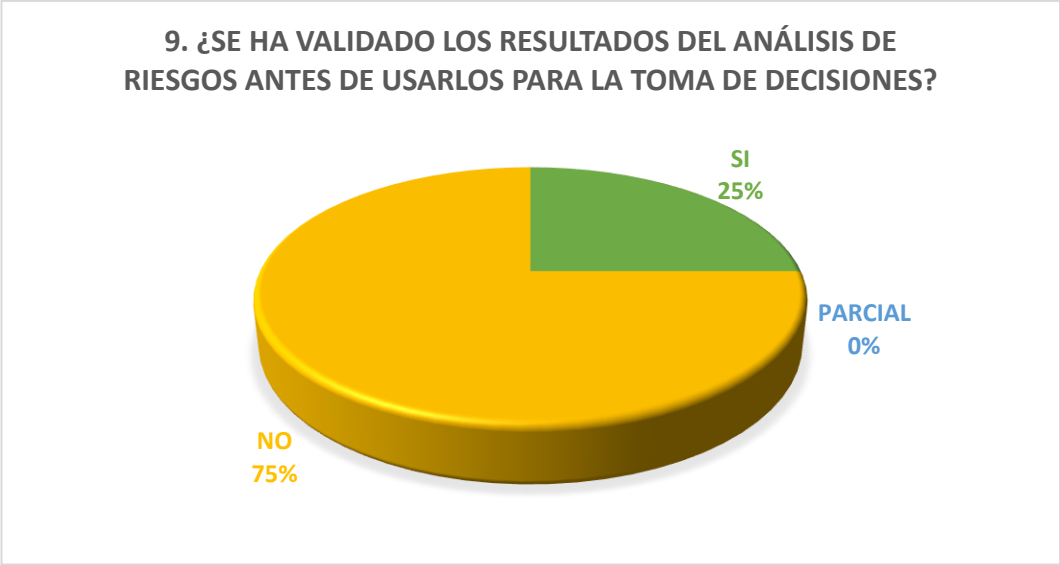


Gráfico 9: ¿Se ha validado los resultados del análisis de riesgos antes de usarlos para la toma de decisiones?

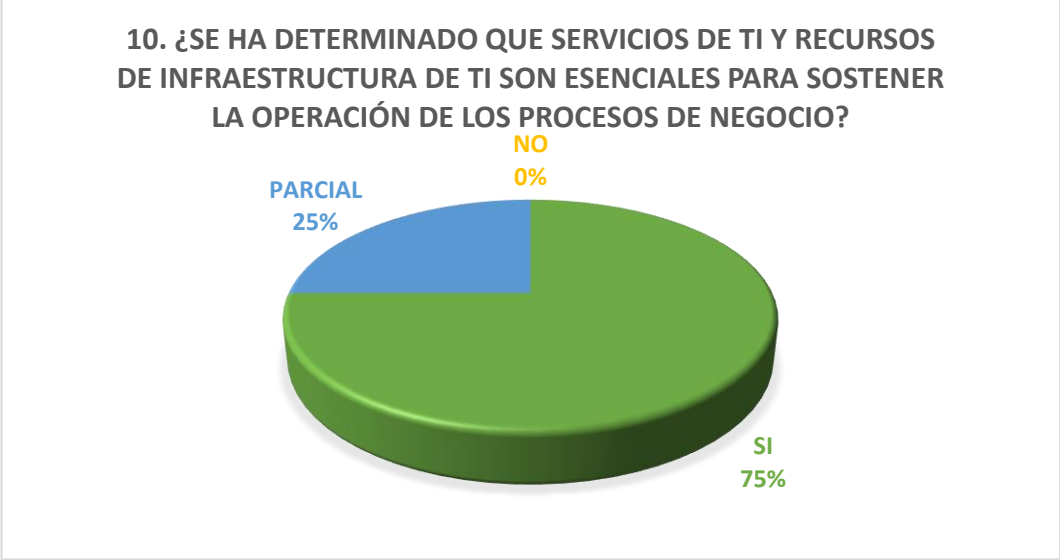


Gráfico 10: ¿Se ha determinado que servicios de TI y recursos de infraestructura de TI son esenciales para sostener la operación de los procesos de negocio?

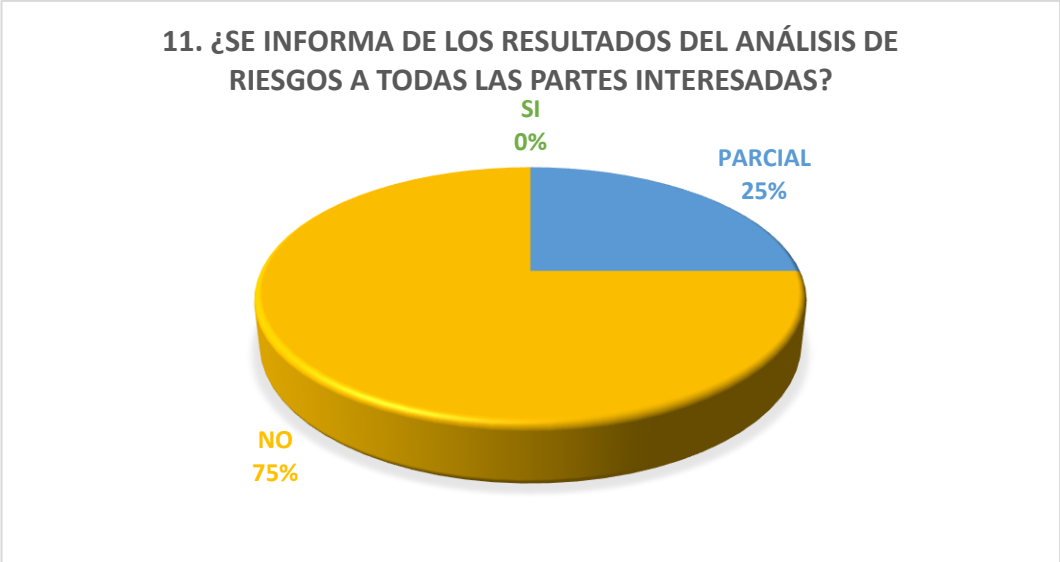


Gráfico 11: ¿Se informa de los resultados del análisis de riesgos a todas las partes interesadas?

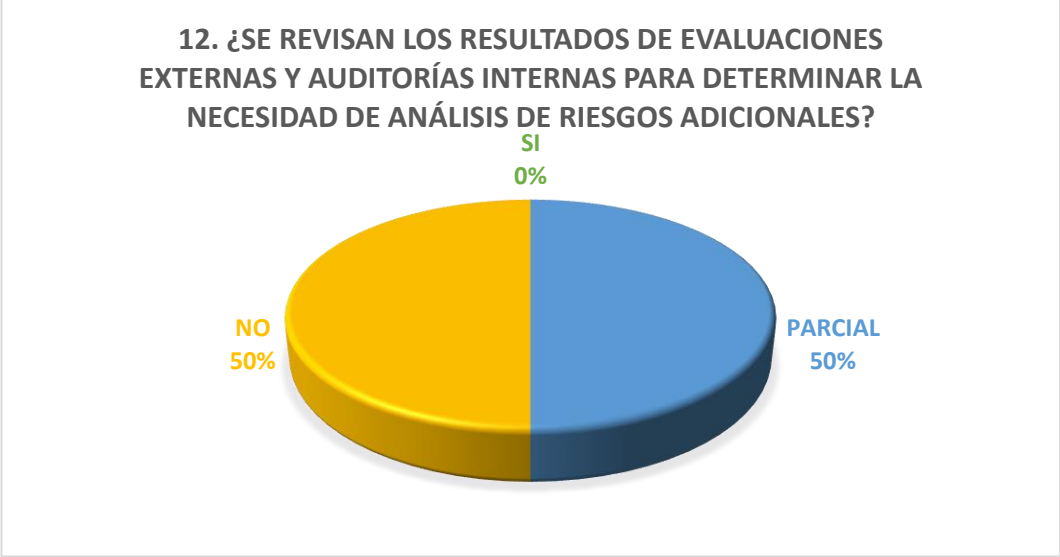


Gráfico 12: ¿Se revisan los resultados de evaluaciones externas y auditorías internas para determinar la necesidad de análisis de riesgos adicionales?

Gráfico 13: ¿Se mantiene un inventario de actividades de control que estén en marcha para gestionar el riesgo?

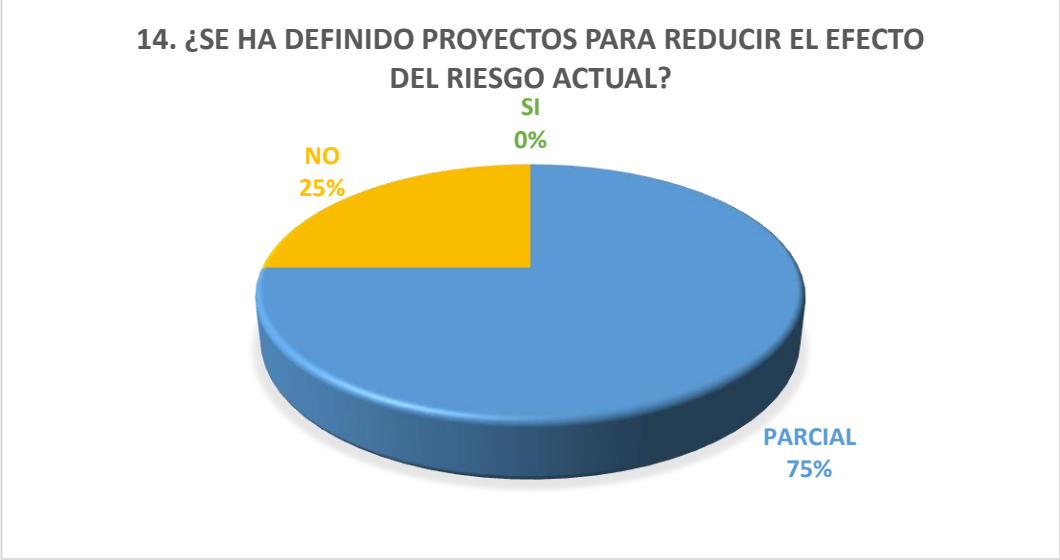


Gráfico 14: ¿Se ha definido proyectos para reducir el efecto del riesgo actual?

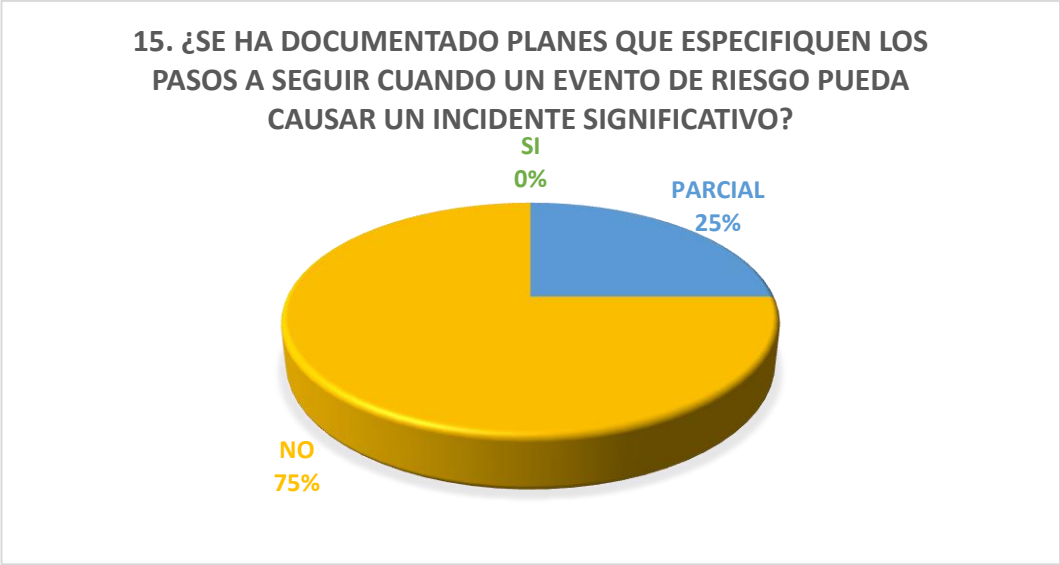


Gráfico 15: ¿Se ha documentado planes que especifiquen los pasos a seguir cuando un evento de riesgo pueda causar un incidente significativo?

ANEXO 4: EJECUCIÓN DEL MODELO DE GESTIÓN DE RIESGOS, ESTUDIO DE CASO EMPRESA AGROINDUSTRIAL ABC

FASE I: DEFINICIÓN DEL ALCANCE, CONTEXTO Y CRITERIOS

1. PASO 01: IDENTIFICAR LOS PROCESOS CRÍTICOS, ÁREAS INVOLUCRADAS Y ACTIVOS

1.1. Procesos críticos

PROCESOS CRÍTICOS EN LA EMPRESA AGROINDUSTRIAL ABC	
CÓDIGO	**PROCESO**
[PRC_001]	Recepción de Arroz Paddy
[PRC_002]	Procesamiento de Arroz Paddy
[PRC_003]	Control de Calidad
[PRC_004]	Control y Gestión de Inventarios
[PRC_005]	Compra de Arroz Paddy
[PRC_006]	Venta de Arroz Blanco y Sub Productos
[PRC_007]	Venta de Servicios de Molinería
[PRC_008]	Gestión Logística de Suministros
[PRC_009]	Gestión de Caja y Bancos
[PRC_010]	Gestión Contable
[PRC_011]	Tecnologías de la Información

Tabla 58: Procesos Críticos en la Empresa Agroindustrial ABC

RPO Y RTO DE PROCESOS CRÍTICOS EN LA EMPRESA AGROINDUSTRIAL ABC			
CÓDIGO	**PROCESO**	**RPO (Horas)**	**RTO (Horas)**
[PRC_001]	Recepción de Arroz Paddy	8 h	4 h
[PRC _002]	Procesamiento de Arroz Paddy	4 h	1 h
[PRC _003]	Control de Calidad	4 h	4 h
[PRC _004]	Control y Gestión de Inventarios	4 h	2 h
[PRC _005]	Compra de Arroz Paddy	4 h	4 h
[PRC _006]	Venta de Arroz Blanco y Sub Productos	4 h	1 h
[PRC _007]	Venta de Servicios de Molinería	4 h	1 h
[PRC _008]	Gestión Logística de Suministros	8 h	4 h
[PRC _009]	Gestión de Caja y Bancos	2 h	1 h
[PRC _010]	Gestión Contable	4 h	2 h
[PRC _011]	Tecnologías de la Información	8 h	1 h

Tabla 59: RPO Y RTO de Procesos Críticos en la Empresa Agroindustrial ABC

1.2. Áreas Involucradas

ÁREAS INVOLUCRADAS EN LOS PROCESOS CRÍTICOS DE LA EMPRESA AGROINDUSTRIAL ABC	
PROCESO CRÍTICO	**ÁREA**
[PRC_001] Recepción de Arroz Paddy	➢ Acopio
[PRC_002] Procesamiento de Arroz Paddy	➢ Producción
[PRC_003] Control de Calidad	➢ Calidad
[PRC _004] Control y Gestión de Inventarios	➢ Acopio ➢ Comercial ➢ Producción
[PRC _005] Compra de Arroz Paddy	➢ Calidad ➢ Comercial ➢ Producción ➢ Tesorería
[PRC _006]	➢ Comercial

ÁREAS INVOLUCRADAS EN LOS PROCESOS CRÍTICOS DE LA EMPRESA AGROINDUSTRIAL ABC	
PROCESO CRÍTICO	**ÁREA**
Venta de Arroz Blanco y Sub Productos	➢ Tesorería
[PRC _007] Venta de Servicios de Molinería	➢ Comercial ➢ Tesorería
[PRC _008] Gestión Logística de Suministros	➢ Logística
[PRC _009] Gestión de Caja y Bancos	➢ Contabilidad ➢ Tesorería
[PRC _010] Gestión Contable	➢ Contabilidad
[PRC _011] Tecnologías de la Información	➢ TI

Tabla 60: Identificación de Áreas Involucradas en los Procesos Críticos de la Empresa Agroindustrial ABC

ÁREAS INVOLUCRADAS
1. Acopio 2. Calidad 3. Comercial 4. Contabilidad 5. Logística 6. Producción 7. Tesorería 8. TI / Sistemas / Informática

Tabla 61: Áreas de Alcance del Proceso de Gestión del Riesgo en la Empresa Agroindustrial ABC

1.3. Activos de Información

ACTIVOS DE INFORMACIÓN DE LA EMPRESA AGROINDUSTRIAL ABC								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
[PRC_001] Recepción de Arroz Paddy	- Archivos informáticos relacionados a la recepción de la materia prima. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel). - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos).	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal del área de acopio).
[PRC_002] Procesamiento de Arroz Paddy	- Archivos informáticos relacionados al procesamiento de la materia prima. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel). - Sistema operativo cliente. - Sistema SCADA (software).	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Sistema SCADA (hardware). - Soporte de la red (switch core, switch desktop, firewall Sophos).	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal del área de producción).

ACTIVOS DE INFORMACIÓN DE LA EMPRESA AGROINDUSTRIAL ABC								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
[PRC_003] Control de Calidad	- Archivos informáticos relacionados al control de la calidad de la materia prima y el producto terminado. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel). - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos).	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal del área de calidad).
[PRC _004] Control y Gestión de Inventarios	- Archivos informáticos relacionados al control y gestión de los inventarios de la materia prima y el producto terminado. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel). - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos, WAP).	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal de las áreas de acopio, comercial y producción).
[PRC _005] Compra de Arroz Paddy	- Archivos informáticos relacionados a la compra de	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales.	- Computadoras. - Servidor de base de datos.	- Internet. - Red local. - VPN.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario.	- Usuarios (personal de las áreas de calidad, comercial,

ACTIVOS DE INFORMACIÓN DE LA EMPRESA AGROINDUSTRIAL ABC								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
	la materia prima. - Base de datos del sistema empresarial.	- Correo electrónico.	- Paquete ofimático (Word, Excel). - Sistema operativo cliente.	- Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos, WAP).	- Wifi.		- UPS.	producción y tesorería).
[PRC _006] Venta de Arroz Blanco y Sub Productos	- Archivos informáticos relacionados a la venta del producto terminado. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales. - Acceso a la web de la empresa. - Correo electrónico.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel, Power Point). - Página web institucional. - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Servidor web. - Soporte de la red (switch core, switch desktop, firewall Sophos, WAP).	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal de las áreas de comercial y tesorería).
[PRC _007] Venta de Servicios de Molinería	- Archivos informáticos relacionados a la venta de servicios de transformación de la materia	- Acceso a las aplicaciones empresariales.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel).	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones.	- Red local.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal de las áreas de comercial y tesorería).

ACTIVOS DE INFORMACIÓN DE LA EMPRESA AGROINDUSTRIAL ABC								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
	prima de clientes. - Base de datos del sistema empresarial.		- Sistema operativo cliente.	- Soporte de la red (switch core, switch desktop, firewall Sophos, WAP).				
[PRC _008] Gestión Logística de Suministros	- Archivos informáticos relacionados a la gestión logística de suministros para los procesos de la empresa. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales. - Correo electrónico.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel). - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos, WAP).	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal del área de logística).
[PRC _009] Gestión de Caja y Bancos	- Archivos informáticos relacionados a la gestión de las operaciones de flujo de dinero. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales. - Correo electrónico.	- Aplicaciones empresariales. - Paquete ofimático (Word, Excel). - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop,	- Internet. - Red local. - VPN. - Wifi.	- Almacenamiento en red. - Documentos impresos.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal de las áreas de contabilidad y tesorería).

ACTIVOS DE INFORMACIÓN DE LA EMPRESA AGROINDUSTRIAL ABC								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
				firewall Sophos, WAP).				
[PRC _010] Gestión Contable	- Archivos informáticos relacionados a la gestión contable de la empresa. - Base de datos del sistema empresarial.	- Acceso a las aplicaciones empresariales. - Acceso a las aplicaciones contables. - Correo electrónico.	- Aplicaciones empresariales. - Aplicaciones contables (CONCAR, PDT). - Paquete ofimático (Word, Excel, Power Point). - Sistema operativo cliente.	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos, WAP).	- Internet. - Red local. - Wifi.	- Almacenamiento en red. - Discos externos. - Documentos impresos. - Memorias USB.	- Fuentes de alimentación. - Mobiliario. - UPS.	- Usuarios (personal del área de contabilidad).
[PRC _011] Tecnologías de la Información	- Base de datos del sistema empresarial. - Código fuente del sistema empresarial. - Copias de respaldo de los archivos, código fuente	- Desarrollo de software in house. - Help Desk. - Soporte técnico de TI.	- IDE de programación. - Paquete ofimático (Word, Excel, Power Point). - Sistema de gestión de base de datos (SQL Server).	- Computadoras. - Servidor de base de datos. - Servidor de aplicaciones. - Soporte de la red (switch core, switch desktop, firewall Sophos).	- Internet. - Red local. - VPN.	- Almacenamiento en red. - Discos externos. - Documentos impresos. - Memorias USB.	- Equipos de climatización (aire acondicionado). - Fuentes de alimentación. - Gabinetes y racks. - Mobiliario. - UPS.	- Administrador de red. - Administrador de sistemas. - Desarrolladores. - Outsourcing.

ACTIVOS DE INFORMACIÓN DE LA EMPRESA AGROINDUSTRIAL ABC								
PROCESO CRÍTICO	**TIPOS DE ACTIVOS**							
	[D] Datos / Información	[S] Servicios	[SW] Software	[HW] Hardware	[COM] Redes de Comunicaciones	[Media] Soportes de Información	[AUX] Equipamiento Auxiliar	[P] Personal
	y base de datos.		- Sistema operativo cliente. - Sistema operativo servidor.					

Tabla 62: Activos de Información por cada Proceso Crítico de la Empresa Agroindustrial ABC

2. PASO 02: IDENTIFICAR EL CONTEXTO EXTERNO E INTERNO

2.1. Contexto Externo

a) Político

Entre las entidades que forman parte del entorno político de la empresa tenemos:

- Estado Peruano.
- Ministerio de Agricultura y Riego (MINAGRI).
- Ministerio de Comercio Exterior y Turismo (MINCETUR).
- Ministerio de la Producción (PRODUCE).
- Ministerio de Economía y Finanzas (MEF).
- Gobiernos Regionales y Locales.
- Gobiernos Internacionales.

Entre las políticas que pueden influir en la empresa tenemos:

- Política Nacional Agraria (PNA).
- Plan Estratégico Nacional Exportador (PENX).
- Estrategia Nacional de Seguridad Alimentaria y Nutricional (ENSAN).
- Política Arancelaria.
- Normas Emitidas por los Gobiernos Regionales y Locales.
- Políticas Internacionales.
- Tratados de Libre Comercio.

b) Legal y Regulatorio

Entre las entidades que forman parte del entorno legal y regulatorio de la empresa tenemos:

- Dirección General de Salud Ambiental (DIGESA)
- Servicio Nacional de Sanidad Agraria (SENASA)
- Instituto Nacional de Calidad (INACAL)
- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
- Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT)

c) Competitivo

- Empresas Molineras de la Región.
- Empresas Molineras del Interior del País.
- Ingreso de Arroz importado.

d) Financiero

Entre las entidades que forman parte del entorno financiero de la empresa tenemos:

- Banco Central de Reserva del Perú (BCRP)
- Banco Agropecuario (AGROBANCO)
- Banco Continental
- Banco de Crédito
- Scotiabank

e) Tecnológico

Conformado por todos los avances tecnológicos o innovaciones técnicas, que pueden contribuir al incremento de la productividad de la empresa cómo, por ejemplo: maquinarias, productos de software, equipos de cómputo, metodologías, estándares, etc. Por otro lado, estos avances tecnológicos también pueden convertirse en objetos o medios

de ataque contra la empresa como, por ejemplo: nuevos virus informáticos, aumento de la ciberdelincuencia, estafas a través de internet, etc.

f) Proveedores

- Proveedores de insumos.
- Proveedores de materia prima (Agricultores, negociantes de arroz, otras empresas molineras).
- Proveedores de servicio de internet (Movistar, Claro).
- Proveedores de servicios de mantenimiento de equipos.
- Proveedores de servicios de transporte.

g) Medioambiental

- Polvo, corrosión y humedad.
- Fenómeno El Niño.
- Fenómeno de La Niña.
- Fenómeno de El Niño Costero.

2.2. Contexto Interno

a) Objetivos Estratégicos

Los objetivos estratégicos de la empresa son presentados a continuación:

- Optimizar la gestión administrativa mediante la implementación de políticas empresariales de planificación y control.
- Implementar la gestión de marketing y ventas para aumentar la participación de mercado.
- Mejorar la eficiencia operacional y logística mediante la optimización de los activos del grupo empresarial.

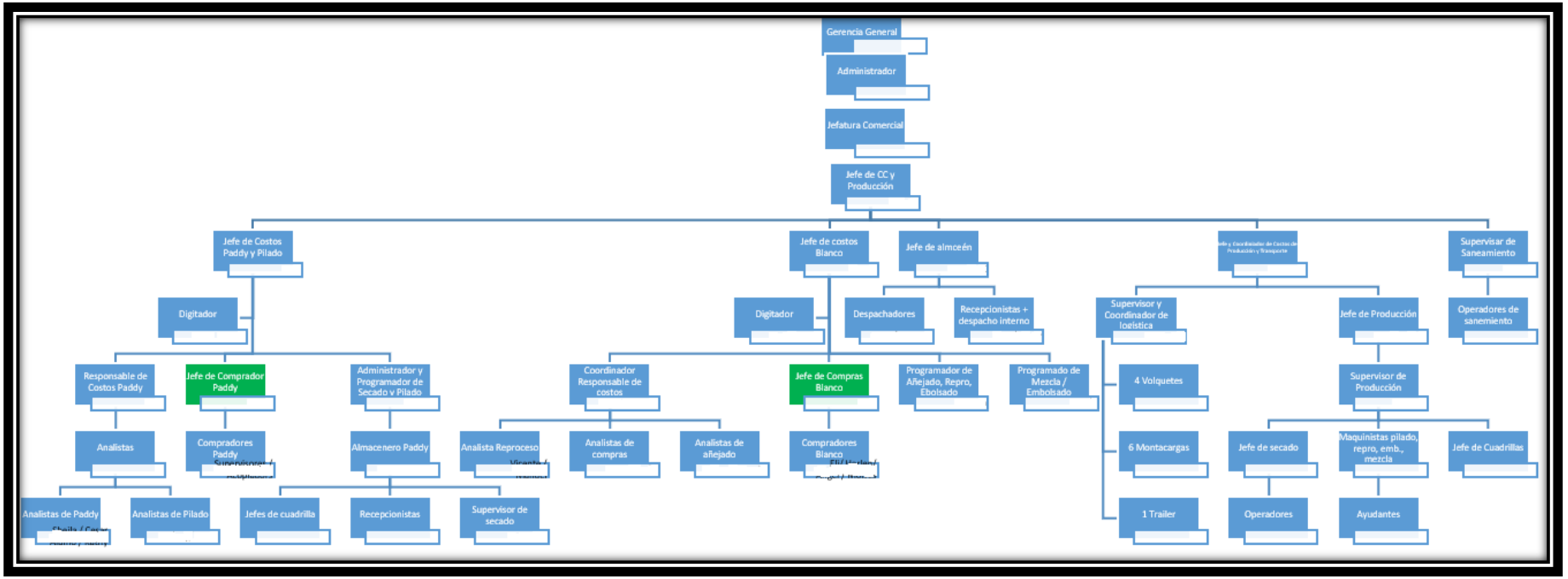
- Incrementar los índices de rentabilidad y mejorar la gestión de indicadores financieros del grupo empresarial.
- Optimizar la gestión de recursos humanos y de organización.
- Implementar un sistema de información integrado para mejorar la gestión de información y toma de decisiones.

b) Política Interna

- Políticas Internas de la Empresa.
- Políticas de Seguridad de la Información.
- Políticas de Seguridad y Salud en el Trabajo.

c) Estructura Organizacional

Figura 10: Organigrama de la Empresa Agroindustrial "ABC"



Fuente: Oficina de RRHH de la Empresa Agroindustrial ABC

d) Procesos:

- [PRC_001] Recepción de Arroz Paddy
- [PRC_002] Procesamiento de Arroz Paddy
- [PRC_003] Control de Calidad
- [PRC_004] Control y Gestión de Inventarios
- [PRC_005] Compra de Arroz Paddy
- [PRC_006] Venta de Arroz Blanco y Sub Productos
- [PRC_007] Venta de Servicios de Molinería
- [PRC_008] Gestión Logística de Suministros
- [PRC_009] Gestión de Caja y Bancos
- [PRC_010] Gestión Contable
- [PRC_011] Tecnologías de la Información

e) Infraestructura Tecnológica

- Aplicaciones empresariales
- Infraestructura de Red
- Equipos Informáticos
- Otros elementos del sistema de información

f) Cultura Organizacional

- Misión: "Brindar productos de calidad, modernizando nuestra industria para obtener una máxima rentabilidad con un alto sentido de responsabilidad y compromiso con el cliente, trabajadores y la sociedad".
- Visión: "Ser a mediano plazo la empresa líder en la comercialización, procesamiento y abastecimiento de arroz en el Perú".
- Valores: Excelencia, Aprendizaje, Proactividad, Responsabilidad y Disciplina.

3. PASO 03: IDENTIFICAR LAS ÁREAS DE IMPACTO DEL RIESGO

DEFINICIÓN Y PONDERACIÓN DE ÁREAS DE IMPACTO DEL RIESGO	
ÁREA DE IMPACTO	**PESO**
Operacional	30%
Reputacional	27%
Financiero	23%
Legal	20%
	Total: 100%

Tabla 63: Identificación y Ponderación de las Áreas de Impacto del Riesgo en la Empresa Agroindustrial ABC

4. PASO 04: DEFINIR ESCALAS DE VALORACIÓN DEL IMPACTO Y LA PROBABILIDAD DEL RIESGO

4.1. Escalas de Impacto

ESCALAS DE IMPACTO OPERACIONAL		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	Más del 80% de las actividades del proceso se ven afectadas.
4	Mayor	Entre el 51% y 80% de las actividades del proceso se ven afectadas.
3	Moderado	Entre el 31% y 50% de las actividades del proceso se ven afectadas.
2	Menor	Entre el 10% y 30% de las actividades del proceso se ven afectadas.
1	Insignificante	Menos del 10% de las actividades del proceso se ven afectadas.

Tabla 64: Escalas de Valoración del Impacto Operacional en la Empresa Agroindustrial ABC

ESCALAS DE IMPACTO REPUTACIONAL		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	La reputación o buena imagen de la empresa está destruida frente a los clientes, proveedores o instituciones externas.
4	Mayor	La reputación o buena imagen de la empresa se ve muy afectada frente a los clientes, proveedores o instituciones externas.
3	Moderado	La reputación o buena imagen de la empresa se ve afectada frente a los clientes, proveedores o instituciones externas.
2	Menor	La reputación o buena imagen de la empresa se ve un poco afectada frente a los clientes, proveedores o instituciones externas.
1	Insignificante	La reputación o buena imagen de la empresa no se ve afectada frente a los clientes, proveedores o instituciones externas. Sin embargo, puede verse afectada dentro de la organización.

Tabla 65: Escalas de Valoración del Impacto Reputacional en la Empresa Agroindustrial ABC

ESCALAS DE IMPACTO FINANCIERO		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	Pérdidas económicas o costos comerciales excepcionalmente elevados; que van desde S/ 1'000,000.00 a más.
4	Mayor	Pérdidas económicas o costos comerciales altamente elevados; que van desde los S/ 300,000.00 hasta S/ 999,999.99.
3	Moderado	Pérdidas económicas o costos comerciales elevados; que van desde los S/ 20,000.00 hasta S/ 299,999.99.
2	Menor	Pérdidas económicas o costos comerciales bajos; que van desde los S/ 5,000.00 hasta S/ 19,999.99.
1	Insignificante	Pérdidas económicas o costos comerciales mínimos; que van desde los S/ 0.00 hasta S/ 4,999.99.

Tabla 66: Escalas de Valoración del Impacto Financiero en la Empresa Agroindustrial ABC

ESCALAS DE IMPACTO LEGAL		
Valor	**Clasificación**	**Descripción**
5	Catastrófico	Incumplimiento excepcionalmente grave de una ley o regulación.
4	Mayor	Incumplimiento grave de una ley o regulación.
3	Moderado	Incumplimiento de una ley o regulación.
2	Menor	Incumplimiento leve o técnico de una ley o regulación.
1	Insignificante	Incumplimiento mínimo o nulo de una ley o regulación.

Tabla 67: Escalas de Valoración del Impacto Legal en la Empresa Agroindustrial ABC

ESCALAS DE IMPACTO TOTAL		
Valor	**Clasificación**	**Impacto Total**
5	Catastrófico	A partir de 3.75
4	Mayor	A partir de 3.50 y menor a 3.75
3	Moderado	A partir de 3.00 y menor a 3.5
2	Menor	A partir de 2.00 y menor a 3.00
1	Insignificante	Menor a 2.00

Tabla 68: Escalas de Valoración del Impacto Total en la Empresa Agroindustrial ABC

4.2. Escalas de Probabilidad

ESCALAS DE PROBABILIDAD		
Valor	**Clasificación**	**Descripción**
5	Casi Seguro	Más de 1 vez al año.
4	Probable	Al menos 1 vez en el último año.
3	Posible	Al menos 1 vez en los últimos 2 años.
2	Poco Probable	Al menos 1 vez en los últimos 5 años.
1	Muy Raro	No se ha presentado en los últimos 5 años.

Tabla 69: Escalas de Valoración de la Probabilidad en la Empresa Agroindustrial ABC

5. PASO 05: DEFINIR CRITERIOS DE ACEPTACIÓN DEL RIESGO

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Casi Seguro	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Posible	3	3	5	9	12	15
Poco Probable	2	2	4	6	8	10
Muy Raro	1	1	2	3	4	5

Tabla 70: Mapa de Calor del Riesgo de la Empresa Agroindustrial ABC

Nivel de Riesgo	Criterio de Aceptación	Descripción
[10 – 25>	Inaceptable	Riesgos que necesitan **MITIGACIÓN**: Planes de actuación **correctivos**.
[5 – 10>	Tolerable	Riesgos que necesitan **INVESTIGACIÓN**: Planes de actuación **preventivos**.
[1 – 5>	Aceptable	Riesgos que necesitan **MONITORIZACIÓN**: Planes de actuación **detectivos**.

Tabla 71: Niveles de Aceptación del Riesgo de la Empresa Agroindustrial ABC

FASE II: EVALUACIÓN DEL RIESGO

6. PASO 06: ELABORAR ESCENARIOS DE RIESGO

ESCENARIOS DE RIESGO DE LOS DATOS

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_001]
Riesgo	Revelación de datos sensibles
Tipo de amenaza	Intencional
Amenaza	Ex – Empleados, Personal interno
Vulnerabilidad	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) de los contratos con el personal.
Escenario negativo	Un empleado o ex - empleado filtra información sensible (relacionada a clientes, proveedores, productos, etc.) a los competidores.
Activos afectados	[D] Datos / Información: archivos informáticos, base de datos.
Procesos afectados	[PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_008] Gestión Logística de Suministros, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Competitivo. Interno: Objetivos estratégicos, política interna, cultura organizacional.
Duración	- Entre el evento y la detección: Largo plazo (semanas). - Efectos del riesgo: Largo plazo (semanas).
Escenario positivo	Los contratos del personal contienen cláusulas de confidencialidad que salvaguardan la información sensible de la empresa.

Tabla 72: Escenario de Riesgo [ESC_RIE_001]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_002]
Riesgo	Corrupción de datos
Tipo de amenaza	No intencional
Amenaza	Personal no capacitado
Vulnerabilidad	Configuración incorrecta de parámetros.
Escenario negativo	El personal configura de manera errónea los parámetros en la aplicación informática, lo cual ocasiona, que se obtengan y registren datos calculados incorrectamente.
Activos afectados	[D] Datos / Información: base de datos.
Procesos afectados	[PRC_003] Control de Calidad, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable,
Contexto influyente	Interno: Política interna, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto a mediano plazo (horas, días).
Escenario positivo	El personal es capacitado en la configuración de parámetros de la aplicación informática, lo que permite que los datos sean calculados correctamente.

Tabla 73: Escenario de Riesgo [ESC_RIE_002]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_003]
Riesgo	Robo de medios de información
Tipo de amenaza	Intencional
Amenaza	Personal deshonesto, visitantes, criminales
Vulnerabilidad	Ausencia de una política sobre limpieza de escritorio y protección de dispositivos de almacenamiento.
Escenario negativo	Personas inescrupulosas sustraen documentos impresos y/o dispositivos electrónicos que contienen información importante para la empresa.
Activos afectados	[D] Datos / Información: archivos informáticos, base de datos. [Media] Soportes de Información: Documentos impresos, discos externos, memorias USB.
Procesos afectados	[PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Competitivo. Interno: Objetivos estratégicos, política interna, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Mediano y largo plazo (días, semanas).
Escenario positivo	Existen políticas y otros controles de protección adecuados para salvaguardar los documentos impresos y los dispositivos electrónicos.

Tabla 74: Escenario de Riesgo [ESC_RIE_003]

ESCENARIOS DE RIESGO DE LAS APLICACIONES

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_004]
Riesgo	Mal funcionamiento del software
Tipo de amenaza	No intencional
Amenaza	Personal (desarrolladores)
Vulnerabilidad	Especificaciones incompletas o no claras para los desarrolladores.
Escenario negativo	Los aplicativos informáticos funcionan incorrectamente, debido a que no se hizo un adecuado levantamiento de requerimientos de los usuarios, generando errores y retrasos en los procesos de negocio.
Activos afectados	[D] Datos / Información: Base de datos, código fuente. [SW] Software: Aplicaciones empresariales.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Tecnológico. Interno: Procesos, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto y mediano plazo (horas, días).
Escenario positivo	Existen procedimientos bien definidos para el levantamiento de requerimientos de software, así como, procedimientos de implementación de los aplicativos informáticos, lo que asegura una correcta puesta en producción.

Tabla 75: Escenario de Riesgo [ESC_RIE_004]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_005]
Riesgo	Abuso de privilegios
Tipo de amenaza	Intencional
Amenaza	Personal malintencionado o negligente
Vulnerabilidad	Ausencia de un procedimiento formal para la revisión de los derechos de acceso de los usuarios.
Escenario negativo	El personal accede indebidamente a los recursos del software ante la presencia de perfiles inadecuados, a través de los cuales, pueden realizar operaciones que no les competen.
Activos afectados	[SW] Software: Aplicaciones empresariales.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Interno: Política interna, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Largo plazo (semanas). - Efectos del riesgo: Mediano y largo plazo (días, semanas).
Escenario positivo	Se realiza una verificación constante de perfiles de acceso y permisos asignados, para asegurar que correspondan a los usuarios correctos.

Tabla 76: Escenario de Riesgo [ESC_RIE_005]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_006]
Riesgo	Repudio de transacciones
Tipo de amenaza	Intencional
Amenaza	Personal deshonesto (usuarios del software)
Vulnerabilidad	Ausencia de pistas de auditoria en los aplicativos informáticos.
Escenario negativo	Se han detectado una serie de operaciones fraudulentas en la aplicación informática y no se puede identificar a los responsables.
Activos afectados	[D] Datos / Información: Base de datos. [SW] Software: Aplicaciones empresariales.
Procesos afectados	[PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Interno: Infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Mediano y largo plazo (días, semanas). - Efectos del riesgo: Corto y mediano plazo (horas, días).
Escenario positivo	Existe un registro apropiado de los eventos en los aplicativos informáticos que permiten la trazabilidad de las actividades que se desarrollan en el mismo.

Tabla 77: Escenario de Riesgo [ESC_RIE_006]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_007]
Riesgo	Ataques de Malware
Tipo de amenaza	Intencional
Amenaza	Pirata informático, criminal informático
Vulnerabilidad	Descarga y uso no controlado de software en las estaciones de trabajo.
Escenario negativo	Se ha producido un ataque de Ransomware, debido a una descarga de software realizada por un usuario, ocasionando la pérdida de archivos importantes.
Activos afectados	[D] Datos / Información: Archivos informáticos. [Media] Soportes de Información: Almacenamiento en red.
Procesos afectados	[PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Tecnológico. Interno: Procesos, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Permanente.
Escenario positivo	Se ha implementado configuraciones que impiden que los usuarios descarguen software no autorizado de internet. Además, se realizan copias de seguridad de los archivos de cada usuario en forma periódica.

Tabla 78: Escenario de Riesgo [ESC_RIE_007]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_008]
Riesgo	Denegación de acciones
Tipo de amenaza	Intencional
Amenaza	Pirata informático
Vulnerabilidad	Deficiente configuración Routers y Firewalls.
Escenario negativo	Se ha producido un ataque distribuido de denegación de servicios (DDoS), que ha provocado la caída de la red e imposibilita el acceso a los aplicativos informáticos.
Activos afectados	[S] Servicios: Acceso a las aplicaciones empresariales, acceso a la web de la empresa. [HW] Hardware: Servidores, Soporte de la red. [COM] Redes de Comunicaciones: Red local.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Competitivo, tecnológico. Interno: Procesos, infraestructura tecnológica.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto plazo (horas).
Escenario positivo	Los dispositivos de red son configurados, de tal modo, que se limita y controla el tráfico de red, reduciendo así la posibilidad de cualquier ataque.

Tabla 79: Escenario de Riesgo [ESC_RIE_008]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_009]
Riesgo	Phishing / Engaños intencionales
Tipo de amenaza	Intencional
Amenaza	Criminal informático, espionaje industrial (otras empresas).
Vulnerabilidad	Falta de conciencia acerca de la seguridad de la información del personal.
Escenario negativo	El personal ha sido víctima de un ataque de Phishing, a través del cual, se ha visto comprometida información sensible de la empresa.
Activos afectados	[D] Datos / Información: Archivos informáticos, contraseñas. [SW] Software: Aplicaciones empresariales. [P] Personal: Usuarios.
Procesos afectados	[PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Competitivo. Interno: Política interna, procesos, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto plazo (horas).
Escenario positivo	El personal recibe capacitación constante acerca de temas relacionados a la seguridad de la información, ataques informáticos, etc.

Tabla 80: Escenario de Riesgo [ESC_RIE_009]

ESCENARIOS DE RIESGO LEGALES Y REGLAMENTARIOS

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_010]
Riesgo	Incumplimiento con contratos de licencias de software
Tipo de amenaza	Intencional
Amenaza	Entidades reguladoras.
Vulnerabilidad	El número de instalaciones de un software propietario sobrepasa el número de licencias adquiridas.
Escenario negativo	La empresa ha recibido una de INDECOPI, debido a la presencia de software propietario instalado sin licencia o que sobrepasa el número instalaciones permitidas.
Activos afectados	[SW] Software: Sistema operativo, paquete ofimático (Word, Excel, Power Point), sistema SCADA (software), software contable, IDE de programación, sistema de gestión de base de datos.
Procesos afectados	[PRC_002] Procesamiento de Arroz Paddy, [PRC_010] Gestión Contable, [PRC_011] Tecnologías de la Información.
Contexto influyente	Externo: Político, Legal y regulatorio, tecnológico, proveedores. Interno: Procesos, política interna, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Mediano y largo plazo (días, semanas).
Escenario positivo	Se han implementado procedimientos que verifican el cumplimiento de disposiciones relacionadas con la propiedad intelectual. Además, se realiza una gestión adecuada del software que se instala en los equipos de trabajo.

Tabla 81: Escenario de Riesgo [ESC_RIE_010]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_011]
Riesgo	Incumplimiento con reglamentos tributarios
Tipo de amenaza	Intencional
Amenaza	Entidades reguladoras
Vulnerabilidad	Ausencia de un módulo o aplicación contable que emita comprobantes electrónicos.
Escenario negativo	La empresa es sancionada por SUNAT al incumplir con la emisión de comprobantes electrónicos, debido a que su aplicación informática no cuenta con dicha funcionalidad.
Activos afectados	[S] Servicios: Acceso a las aplicaciones contables.
Procesos afectados	[PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_010] Gestión Contable.
Contexto influyente	Externo: Político, legal y regulatorio, tecnológico, proveedores. Interno: Procesos, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Mediano y largo plazo (días, semanas).
Escenario positivo	Se han implementado funciones contables en la aplicación informática de la empresa, de tal forma, que se cumplen los reglamentos relacionados con la emisión de comprobantes electrónicos.

Tabla 82: Escenario de Riesgo [ESC_RIE_011]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_012]
Riesgo	Daño a los equipos informáticos
Tipo de amenaza	Naturales
Amenaza	Polvo, corrosión, humedad
Vulnerabilidad	Susceptibilidad al polvo, corrosión y humedad.
Escenario negativo	Los equipos informáticos de la empresa se ven dañados debido a que no se han implementado las medidas de protección físicas adecuadas.
Activos afectados	[HW] Hardware: Computadoras, servidores, sistema SCADA (hardware), soporte de la red.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable, [PRC_011] Tecnologías de la Información.
Contexto influyente	Externo: Medioambiental. Interno: Procesos, infraestructura tecnológica.
Duración	- Entre el evento y la detección: Largo plazo (semanas). - Efectos del riesgo: Corto y mediano plazo (horas, días).
Escenario positivo	Se realizan mantenimientos preventivos constantemente y se han implementado medidas de protección ante factores ambientales propios del negocio.

Tabla 83: Escenario de Riesgo [ESC_RIE_012]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_013]
Riesgo	Destrucción de servidores y otros equipos informáticos
Tipo de amenaza	No intencional
Amenaza	Incendio
Vulnerabilidad	Ubicación en área susceptible de incendios.
Escenario negativo	Se produce un incendio en el taller de mantenimiento, el cual está ubicado al costado del área donde se encuentran los servidores de la empresa. Como consecuencia de esto, los servidores y otros equipos informáticos fueron destruidos.
Activos afectados	[D] Datos / Información: Archivos informáticos, base de datos, código fuente. [S] Servicios: Acceso a las aplicaciones empresariales, acceso a la web de la empresa. [HW] Hardware: Servidores, computadoras, soporte de la red. [COM] Redes de Comunicaciones: Internet, red local, VPN, wifi. [Media] Soportes de Información: Almacenamiento en red. [AUX] Equipamiento Auxiliar: Equipos de climatización, fuentes de alimentación, mobiliario, UPS.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable, [PRC_011] Tecnologías de la Información.
Contexto influyente	Interno: Procesos, infraestructura tecnológica.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Largo plazo (semanas), permanente.
Escenario positivo	El centro de datos ha sido ubicado en un ambiente alejado de áreas susceptibles a un siniestro de incendio. Además, se han implementado medidas de seguridad como aspersores, extintores, etc.

Tabla 84: Escenario de Riesgo [ESC_RIE_013]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_014]
Riesgo	Robo de equipos
Tipo de amenaza	Intencional
Amenaza	Personal deshonesto, visitantes
Vulnerabilidad	Ausencia de protección física de la edificación (paredes, puertas y ventanas) y dispositivos de videovigilancia.
Escenario negativo	Se han extraído ilícitamente equipos informáticos de las instalaciones de la empresa. Además, los implicados no pueden ser identificados debido a la ausencia de registros en videos.
Activos afectados	[D] Datos / Información: archivos informáticos. [HW] Hardware: Computadoras, soporte de la red.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios.
Contexto influyente	Interno: Política interna, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto plazo (horas).
Escenario positivo	La edificación presenta paredes, puertas y ventanas que resguardan los equipos de cada oficina. Además, se han implementado dispositivos de videovigilancia y protocolos de ingreso y salida del personal y visitantes.

Tabla 85: Escenario de Riesgo [ESC_RIE_014]

ESCENARIOS DE RIESGO DEL ENTORNO FÍSICO

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_015]
Riesgo	Infiltración de agua de lluvia
Tipo de amenaza	Naturales
Amenaza	Fenómeno de "El Niño"
Vulnerabilidad	Ubicación de instalaciones en áreas susceptibles de inundación.
Escenario negativo	Se han presentado intensas lluvias que han afectado a varios componentes físicos del sistema de información, debido a que los ambientes donde se encontraban alojados presentaban deficiencias por donde se infiltró el agua de lluvia.
Activos afectados	[HW] Hardware: Computadoras, soporte de la red. [COM] Redes de Comunicaciones: Red local. [Media] Soportes de Información: Documentos impresos.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_004] Control y Gestión de Inventarios, [PRC_008] Gestión Logística de Suministros.
Contexto influyente	Externo: Medioambiental. Interno: Procesos, infraestructura tecnológica, cultura organizacional.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto y mediano plazo (horas, días).
Escenario positivo	Los ambientes han sido acondicionados adecuadamente para evitar cualquier infiltración de agua de lluvia.

Tabla 86: Escenario de Riesgo [ESC_RIE_015]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_016]
Riesgo	Fallas de energía eléctrica
Tipo de amenaza	No intencional
Amenaza	Red energética inestable
Vulnerabilidad	Susceptibilidad de los equipos informáticos a las variaciones de voltaje.
Escenario negativo	El suministro eléctrico presenta variaciones de voltaje que afectan a los equipos informáticos, causando interrupciones en las operaciones diarias de la empresa.
Activos afectados	[HW] Hardware: Computadoras, servidores, soporte de la red. [COM] Redes de Comunicaciones: Red local.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable, [PRC_011] Tecnologías de la Información.
Contexto influyente	Interno: Procesos, infraestructura tecnológica.
Duración	- Entre el evento y la detección: Corto plazo (horas). - Efectos del riesgo: Corto plazo (horas).
Escenario positivo	Se disponen de dispositivos UPS que permiten que las operaciones continúen por un tiempo limitado al ocurrir un apagón eléctrico. Además, se cuenta con fuentes de alimentación que protegen a los equipos informáticos de la variación de voltaje

Tabla 87: Escenario de Riesgo [ESC_RIE_016]

ESCENARIOS DE RIESGO DEL PERSONAL

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_017]
Riesgo	Desconocimiento del usuario
Tipo de amenaza	No intencional
Amenaza	Personal no capacitado
Vulnerabilidad	Ausencia de procedimientos de inducción al personal en el uso de los aplicativos informáticos.
Escenario negativo	Los usuarios del sistema cometen errores al realizar el registro de sus operaciones, afectando a la información del negocio y causando errores de otras áreas que hacen uso de esta información.
Activos afectados	[D] Datos / Información: Base de datos. [SW] Software: Aplicaciones empresariales. [P] Personal: Usuarios.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Interno: Objetivos estratégicos, política interna, cultura organizacional.
Duración	- Entre el evento y la detección: Corto y mediano plazo (horas, días). - Efectos del riesgo: Corto y mediano plazo (horas, días).
Escenario positivo	Se cuenta con procedimientos de inducción adecuados y manuales de usuario bien detallados para el nuevo personal que ingresa a la empresa.

Tabla 88: Escenario de Riesgo [ESC_RIE_017]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_018]
Riesgo	Negligencia de los usuarios al utilizar los aplicativos informáticos
Tipo de amenaza	Intencional
Amenaza	Personal negligente
Vulnerabilidad	Ausencia de responsabilidades en seguridad de la información en la descripción de los cargos.
Escenario negativo	El personal realiza el registro de sus operaciones sin seguir los procedimientos indicados en el manual de usuario, cometiendo continuamente los mismos errores, a pesar de ser capacitados en reiteradas ocasiones.
Activos afectados	[D] Datos / Información: Base de datos. [S] Servicios: Help Desk. [P] Personal: Usuarios.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable.
Contexto influyente	Interno: Procesos, política interna, cultura organizacional.
Duración	- Entre el evento y la detección: Mediano y largo plazo (días, semanas). - Efectos del riesgo: Mediano y largo plazo (días, semanas).
Escenario positivo	Existen políticas de seguridad de la información donde se definen responsabilidades y sanciones a los usuarios con respecto a la utilización y registro de la información que tienen a su cargo, evitando así, que cometan actos de negligencia al realizar sus actividades.

Tabla 89: Escenario de Riesgo [ESC_RIE_018]

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_019]
Riesgo	Habilidades inadecuadas del personal de TI
Tipo de amenaza	No intencional
Amenaza	Personal de TI (programadores)
Vulnerabilidad	Ausencia de procedimientos para evaluar correctamente las habilidades del personal de TI.
Escenario negativo	Se producen fallas durante el uso de las aplicaciones informáticas, debido a que los programadores no implementaron medidas de gestión de excepciones al desarrollar el software.
Activos afectados	[D] Datos / Información: Base de datos, código fuente. [S] Servicios: Desarrollo de software. [SW] Software: Aplicaciones empresariales. [P] Personal: Usuarios.
Procesos afectados	[PRC_001] Recepción de Arroz Paddy, [PRC_002] Procesamiento de Arroz Paddy, [PRC_003] Control de Calidad, [PRC_004] Control y Gestión de Inventarios, [PRC_005] Compra de Arroz Paddy, [PRC_006] Venta de Arroz Blanco y Sub Productos, [PRC_007] Venta de Servicios de Molinería, [PRC_008] Gestión Logística de Suministros, [PRC_009] Gestión de Caja y Bancos, [PRC_010] Gestión Contable, [PRC_011] Tecnologías de la Información.
Contexto influyente	Externo: Tecnológico. Interno: Objetivos estratégicos, política interna, procesos, cultura organizacional.
Duración	- Entre el evento y la detección: Mediano y largo plazo (días, semanas). - Efectos del riesgo: Mediano y largo plazo (días, semanas).
Escenario positivo	Los desarrolladores han pasado por un riguroso y adecuado proceso de evaluación antes de ser contratados, asegurando que poseen las competencias necesarias para el cargo. Además, reciben capacitaciones constantes acerca de buenas prácticas de desarrollo de software, obteniendo así, productos de software de calidad.

Tabla 90: Escenario de Riesgo [ESC_RIE_019]

ESCENARIOS DE RIESGO DE LOS PROVEEDORES, TERCEROS Y OUTSOURCING

DEFINICIÓN DEL ESCENARIO DE RIESGO	
Código	[ESC_RIE_020]
Riesgo	Nivel de servicio bajo
Tipo de amenaza	Intencional
Amenaza	Proveedores, outsourcing
Vulnerabilidad	Ausencia de acuerdos de nivel de servicio (SLAs).
Escenario negativo	Se han presentado fallas en el funcionamiento y rendimiento de la infraestructura tecnológica, los cuales no han sido solucionados a tiempo por los proveedores de servicios de TI, generando retrasos en las operaciones de los usuarios.
Activos afectados	[S] Servicios: Acceso a las aplicaciones empresariales, Acceso a las aplicaciones contables, acceso a la web de la empresa, correo electrónico, desarrollo de software, help desk, soporte técnico.
Procesos afectados	Recepción de Arroz Paddy, Procesamiento de Arroz Paddy, Control de Calidad, Control y Gestión de Inventarios, Compra de Arroz Paddy, Venta de Arroz Blanco y Sub Productos, Venta de Servicios de Molinería, Gestión Logística de Suministros, Gestión de Caja y Bancos, Gestión Contable, Tecnologías de la Información.
Contexto influyente	Externo: Proveedores. Interno: Política interna, procesos, infraestructura tecnológica.
Duración	- Entre el evento y la detección: Corto y mediano plazo (horas, días). - Efectos del riesgo: Corto y mediano plazo (horas, días).
Escenario positivo	Existen acuerdos de nivel de servicio (SLAs) adecuados suscritos entre la empresa y el proveedor de servicios de TI, asegurando que cualquier inconveniente sea solucionado a tiempo, impactando mínimamente en las operaciones.

Tabla 91: Escenario de Riesgo [ESC_RIE_020]

7. PASO 07: CALCULAR Y VALORAR EL RIESGO INHERENTE

N°	Escenario de Riesgo		Impacto						Probabilidad (P)	Nivel de Riesgo (I * P)	Criterio de Aceptación
	Código	Riesgo	Impacto Operacional (0.30)	Impacto Reputacional (0.27)	Impacto Financiero (0.23)	Impacto Legal (0.20)	Impacto Total	Impacto (I)			
1	[ESC_RIE_001]	Revelación de datos sensibles	3	4	4	3	3.50	4	3	12	Inaceptable
2	[ESC_RIE_002]	Corrupción de datos	3	3	2	2	2.57	2	5	10	Inaceptable
3	[ESC_RIE_003]	Robo de medios de información	4	3	3	2	3.10	3	3	9	Tolerable
4	[ESC_RIE_004]	Mal funcionamiento del software	4	3	2	2	2.87	2	5	10	Inaceptable
5	[ESC_RIE_005]	Abuso de privilegios	4	2	2	1	2.40	2	5	10	Inaceptable
6	[ESC_RIE_006]	Repudio de transacciones	4	2	3	3	3.03	3	2	6	Tolerable
7	[ESC_RIE_007]	Ataques de Malware	4	3	3	2	3.10	3	3	9	Tolerable
8	[ESC_RIE_008]	Denegación de acciones	5	3	2	2	3.17	3	2	6	Tolerable
9	[ESC_RIE_009]	Phishing / Engaños intencionales	3	3	4	2	3.03	3	4	12	Inaceptable
10	[ESC_RIE_010]	Incumplimiento con contratos de licencias de software	5	4	3	4	4.07	5	3	15	Inaceptable
11	[ESC_RIE_011]	Incumplimiento con reglamentos tributarios	5	4	4	4	4.30	5	2	10	Inaceptable
12	[ESC_RIE_012]	Daño a los equipos informáticos	4	2	3	1	2.63	2	5	10	Inaceptable
13	[ESC_RIE_013]	Destrucción de servidores y otros equipos informáticos	5	3	4	2	3.63	4	3	12	Inaceptable
14	[ESC_RIE_014]	Robo de equipos	3	3	2	1	2.37	2	4	8	Tolerable
15	[ESC_RIE_015]	Infiltración de agua de lluvia	4	3	2	1	2.67	2	3	6	Tolerable
16	[ESC_RIE_016]	Fallas de energía eléctrica	4	3	2	1	2.67	2	5	10	Inaceptable
17	[ESC_RIE_017]	Desconocimiento del usuario	4	3	1	1	2.44	2	5	10	Inaceptable

N°	Escenario de Riesgo		Impacto						Probabilidad (P)	Nivel de Riesgo (I * P)	Criterio de Aceptación
	Código	Riesgo	Impacto Operacional (0.30)	Impacto Reputacional (0.27)	Impacto Financiero (0.23)	Impacto Legal (0.20)	Impacto Total	Impacto (I)			
18	[ESC_RIE_018]	Negligencia de los usuarios al utilizar los aplicativos informáticos	4	3	2	2	2.87	2	5	10	Inaceptable
19	[ESC_RIE_019]	Habilidades inadecuadas del personal de TI	4	2	2	2	2.60	2	3	6	Tolerable
20	[ESC_RIE_020]	Nivel de servicio bajo	4	3	2	2	2.87	2	5	10	Inaceptable

Tabla 92: Cálculo y Valoración del Riesgo Inherente de la Empresa Agroindustrial ABC

FASE III: TRATAMIENTO DEL RIESGO

8. PASO 08: DEFINIR OPCIONES DE TRATAMIENTO DEL RIESGO

Las opciones de tratamiento del riesgo que pueden ser consideradas por la empresa son las siguientes:

- Aceptar el Riesgo
- Mitigar el Riesgo
- Compartir el Riesgo
- Evitar el Riesgo

9. PASO 09: CALCULAR Y VALORAR EL RIESGO RESIDUAL

ESCENARIOS DE RIESGO DE LOS DATOS

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_001]					
Riesgo	Revelación de datos sensibles					
Tipo de Amenaza	Intencional					
Amenaza	Ex – Empleados, Personal interno					
Vulnerabilidad	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) de los contratos con el personal.					
Escenario Negativo	Un empleado o ex - empleado filtra información sensible (relacionada a clientes, proveedores, productos, etc.) a los competidores.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	3.50	4	3	12	**Inaceptable**
Reputacional (0.27)	4					
Financiero (0.23)	4					
Legal (0.20)	3					

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO			
OPCIONES DE TRATAMIENTO DEL RIESGO			
Aceptar	**Mitigar**	**Compartir**	**Evitar**
Si ha seleccionado mitigar o compartir el riesgo:			
¿Qué salvaguardas aplicaría?			**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**
Salvaguardas Existentes	**Salvaguardas a Implementar**		
- Ninguna.	- Cláusulas de confidencialidad en los contratos de trabajo. - Soluciones Data Loss Prevention (DLP).		Probabilidad

NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	3.50	4	1	4	**Aceptable**
Reputacional (0.27)	4					
Financiero (0.23)	4					
Legal (0.20)	3					

Tabla 93: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_001]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_002]					
Riesgo	Corrupción de datos					
Tipo de Amenaza	No intencional					
Amenaza	Personal no capacitado					
Vulnerabilidad	Configuración incorrecta de parámetros.					
Escenario Negativo	El personal configura de manera errónea los parámetros en la aplicación informática, lo cual ocasiona, que se obtengan y registren datos calculados incorrectamente.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	2.57	2	5	10	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Inducciones cortas brindadas por el área de TI al nuevo personal.	- Capacitaciones constantes a todos los usuarios sobre el uso correcto de los aplicativos informáticos. - Desarrollo y actualización periódica de los manuales de usuario.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	2.57	2	3	6	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					

Tabla 94: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_002]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_003]					
Riesgo	Robo de medios de información					
Tipo de Amenaza	Intencional					
Amenaza	Personal deshonesto, visitantes, criminales					
Vulnerabilidad	Ausencia de una política sobre limpieza de escritorio y protección de dispositivos de almacenamiento.					
Escenario Negativo	Personas inescrupulosas sustraen documentos impresos y/o dispositivos electrónicos que contienen información importante para la empresa.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	3.10	3	3	9	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	3					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Ninguna.	- Política sobre el uso de dispositivos externos. - Política de escritorio limpio.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	3.10	3	1	3	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	3					
Legal (0.20)	2					

Tabla 95: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_003]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_004]					
Riesgo	Mal funcionamiento del software					
Tipo de Amenaza	No intencional					
Amenaza	Personal (desarrolladores)					
Vulnerabilidad	Especificaciones incompletas o no claras para los desarrolladores.					
Escenario Negativo	Los aplicativos informáticos funcionan incorrectamente, debido a que no se hizo un adecuado levantamiento de requerimientos de los usuarios, generando errores y retrasos en los procesos de negocio.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.87	2	5	10	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Ninguna.	- Metodología de desarrollo de software (gestión de requerimientos). - Procedimientos para la implantación de aplicaciones.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.87	2	2	4	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					

Tabla 96: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_004]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_005]					
Riesgo	Abuso de privilegios					
Tipo de Amenaza	Intencional					
Amenaza	Personal malintencionado o negligente					
Vulnerabilidad	Ausencia de un procedimiento formal para la revisión de los derechos de acceso de los usuarios.					
Escenario Negativo	El personal accede indebidamente a los recursos del software ante la presencia de perfiles inadecuados, a través de los cuales, pueden realizar operaciones que no les competen.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.40	2	5	10	**Inaceptable**
Reputacional (0.27)	2					
Financiero (0.23)	2					
Legal (0.20)	1					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?				**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**		
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Ninguna.	- Gestión adecuada de accesos y perfiles de usuario.			Probabilidad		
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.40	2	2	4	**Aceptable**
Reputacional (0.27)	2					
Financiero (0.23)	2					
Legal (0.20)	1					

Tabla 97: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_005]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_006]					
Riesgo	Repudio de transacciones					
Tipo de Amenaza	Intencional					
Amenaza	Personal deshonesto (usuarios del software)					
Vulnerabilidad	Ausencia de pistas de auditoria en los aplicativos informáticos.					
Escenario Negativo	Se han detectado una serie de operaciones fraudulentas en la aplicación informática y no se puede identificar a los responsables.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	3.03	3	2	6	**Tolerable**
Reputacional (0.27)	2					
Financiero (0.23)	3					
Legal (0.20)	3					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?			**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**			
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Ninguna.	- Tablas y campos de auditoria en la base de datos de los aplicativos informáticos.		Probabilidad			
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	3.03	3	1	3	**Aceptable**
Reputacional (0.27)	2					
Financiero (0.23)	3					
Legal (0.20)	3					

Tabla 98: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_006]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_007]					
Riesgo	Ataques de Malware					
Tipo de Amenaza	Intencional					
Amenaza	Pirata informático, criminal informático					
Vulnerabilidad	Descarga y uso no controlado de software en las estaciones de trabajo.					
Escenario Negativo	Se ha producido un ataque de Ransomware, debido a una descarga de software realizada por un usuario, ocasionando la pérdida de archivos importantes.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	3.10	3	3	9	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	3					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Antivirus.	- Configuración de firewall. - Actualizaciones del sistema operativo y aplicaciones. Filtro antispam.				Probabilidad	
	- Copias de seguridad diarias.				Impacto	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	1	1.74	1	1	1	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	1					
Legal (0.20)	2					

Tabla 99: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_007]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_008]					
Riesgo	Denegación de acciones					
Tipo de Amenaza	Intencional					
Amenaza	Pirata informático					
Vulnerabilidad	Deficiente configuración Routers y Firewalls.					
Escenario Negativo	Se ha producido un ataque distribuido de denegación de servicios (DDoS), que ha provocado la caída de la red e imposibilita el acceso a los aplicativos informáticos.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	3.17	3	2	6	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**		**Compartir**		**Evitar**	
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes		**Salvaguardas a Implementar**				
- Monitorear las IPs que están accediendo al servidor.		- Contratar servicios de proveedor de Internet o hosting web especializados en protección DDoS.			**Probabilidad**	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	3.17	3	1	3	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					

Tabla 100: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_008]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_009]					
Riesgo	Phishing / Engaños intencionales					
Tipo de Amenaza	Intencional					
Amenaza	Criminal informático, espionaje industrial (otras empresas).					
Vulnerabilidad	Falta de conciencia acerca de la seguridad de la información del personal.					
Escenario Negativo	El personal ha sido víctima de un ataque de Phishing, a través del cual, se ha visto comprometida información sensible de la empresa.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	3.03	3	4	12	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	4					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Antivirus.	- Concientización en cultura de seguridad de la información para el personal. - Plan de seguridad Anti-Phishing.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	3.03	3	2	6	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	4					
Legal (0.20)	2					

Tabla 101: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_009]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_010]					
Riesgo	Incumplimiento con contratos de licencias de software					
Tipo de Amenaza	Intencional					
Amenaza	Entidades reguladoras					
Vulnerabilidad	El número de instalaciones de un software propietario sobrepasa el número de licencias adquiridas.					
Escenario Negativo	La empresa ha recibido una multa de INDECOPI, debido a la presencia de software propietario instalado sin licencia o que sobrepasa el número instalaciones permitidas.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	4.07	5	3	15	**Inaceptable**
Reputacional (0.27)	4					
Financiero (0.23)	3					
Legal (0.20)	4					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Gestión de software instalado en cada computadora.	- Adquisición de licencias de software de sistema operativo y paquete ofimático. - Utilizar software libre para las actividades de TI.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	4.07	5	1	5	**Tolerable**
Reputacional (0.27)	4					
Financiero (0.23)	3					
Legal (0.20)	4					

Tabla 102: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_010]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_011]					
Riesgo	Incumplimiento con reglamentos tributarios					
Tipo de Amenaza	Intencional					
Amenaza	Entidades reguladoras					
Vulnerabilidad	Ausencia de un módulo o aplicación contable que emita comprobantes electrónicos.					
Escenario Negativo	La empresa es sancionada por SUNAT al incumplir con la emisión de comprobantes electrónicos, debido a que su aplicación informática no cuenta con dicha funcionalidad.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	4.30	5	2	10	**Inaceptable**
Reputacional (0.27)	4					
Financiero (0.23)	4					
Legal (0.20)	4					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**		**Compartir**		**Evitar**	
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes		**Salvaguardas a Implementar**				
- Funcionalidades de emisión de comprobantes electrónicos en el sistema de la empresa.		- Contratar un Operador de Servicios Electrónicos (OSE) para la verificación de sus comprobantes electrónicos.			Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	4.30	5	1	5	**Tolerable**
Reputacional (0.27)	4					
Financiero (0.23)	4					
Legal (0.20)	4					

Tabla 103: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_011]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_012]					
Riesgo	Daño a los equipos informáticos					
Tipo de Amenaza	Naturales					
Amenaza	Polvo, corrosión, humedad					
Vulnerabilidad	Susceptibilidad al polvo, corrosión y humedad.					
Escenario Negativo	Los equipos informáticos de la empresa se ven dañados debido a que no se han implementado las medidas de protección físicas adecuadas.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.63	2	5	10	**Inaceptable**
Reputacional (0.27)	2					
Financiero (0.23)	3					
Legal (0.20)	1					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Mantenimiento correctivo de equipos informáticos.	- Mantenimiento preventivo de equipos informáticos. - Medidas de protección física.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.63	2	2	4	**Aceptable**
Reputacional (0.27)	2					
Financiero (0.23)	3					
Legal (0.20)	1					

Tabla 104: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_012]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_013]					
Riesgo	Destrucción de servidores y otros equipos informáticos					
Tipo de Amenaza	No intencional					
Amenaza	Incendio					
Vulnerabilidad	Ubicación en área susceptible de incendios.					
Escenario Negativo	Se produce un incendio en el taller de mantenimiento, el cual está ubicado al costado del área donde se encuentran los servidores de la empresa. Como consecuencia de esto, los servidores y otros equipos informáticos fueron destruidos.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	3.63	4	3	12	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	4					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?				**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**		
Salvaguardas Existentes		**Salvaguardas a Implementar**				
- Extintores.		- Reubicación del centro de datos.		Probabilidad		
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	5	3.63	4	1	4	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	4					
Legal (0.20)	2					

Tabla 105: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_013]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_014]					
Riesgo	Robo de equipos					
Tipo de Amenaza	Intencional					
Amenaza	Personal deshonesto, visitantes					
Vulnerabilidad	Ausencia de protección física de la edificación (paredes, puertas y ventanas) y dispositivos de videovigilancia.					
Escenario Negativo	Se han extraído ilícitamente equipos informáticos de las instalaciones de la empresa. Además, los implicados no pueden ser identificados debido a la ausencia de registros en videos.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	2.37	2	4	8	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	1					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?				**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**		
Salvaguardas Existentes		**Salvaguardas a Implementar**				
- Cámaras de seguridad en oficinas y otros ambientes.		- Políticas de ingreso y salida del personal y otros visitantes.		Probabilidad		
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	3	2.37	2	**1**	**2**	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	1					

Tabla 106: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_014]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_015]					
Riesgo	Infiltración de agua de lluvia					
Tipo de Amenaza	Naturales					
Amenaza	Fenómeno de "El Niño"					
Vulnerabilidad	Ubicación de instalaciones en áreas susceptibles de inundación.					
Escenario Negativo	Se han presentado intensas lluvias que han afectado a varios componentes físicos del sistema de información, debido a que los ambientes donde se encontraban alojados presentaban deficiencias por donde se infiltró el agua de lluvia.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.67	2	3	6	**Tolerable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	1					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**		**Compartir**		**Evitar**	
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Ninguna.	- Acondicionar los ambientes para evitar la infiltración. - Protección física de los equipos.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.67	2	2	4	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	1					

Tabla 107: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_015]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO	
ESCENARIO DE RIESGO	
Código	[ESC_RIE_016]
Riesgo	Fallas de energía eléctrica
Tipo de Amenaza	No intencional
Amenaza	Red energética inestable
Vulnerabilidad	Susceptibilidad de los equipos informáticos a las variaciones de voltaje.
Escenario Negativo	El suministro eléctrico presenta variaciones de voltaje que afectan a los equipos informáticos, causando interrupciones en las operaciones diarias de la empresa.

NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.67	2	5	10	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	1					

OPCIONES DE TRATAMIENTO DEL RIESGO			
Aceptar	**Mitigar**	**Compartir**	**Evitar**

Si ha seleccionado mitigar o compartir el riesgo:		
¿Qué salvaguardas aplicaría?		**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**
Salvaguardas Existentes	**Salvaguardas a Implementar**	
- UPS para los servidores. - Estabilizadores de voltaje.	- Equipos UPS para computadoras.	Probabilidad

NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.67	2	2	4	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	1					

Tabla 108: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_016]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_017]					
Riesgo	Desconocimiento del usuario					
Tipo de Amenaza	No intencional					
Amenaza	Personal no capacitado					
Vulnerabilidad	Ausencia de procedimientos de inducción al personal en el uso de los aplicativos informáticos.					
Escenario Negativo	Los usuarios del sistema cometen errores al realizar el registro de sus operaciones, afectando a la información del negocio y causando errores de otras áreas que hacen uso de esta información.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.44	2	5	10	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	1					
Legal (0.20)	1					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?						**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Manuales de usuario básicos.	- Manuales de usuario por procesos de negocio. - Proceso de inducción adecuado en procesos y aplicativos informáticos.					Probabilidad
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.44	2	2	4	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	1					
Legal (0.20)	1					

Tabla 109: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_017]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO	
ESCENARIO DE RIESGO	
Código	[ESC_RIE_018]
Riesgo	Negligencia de los usuarios al utilizar los aplicativos informáticos
Tipo de Amenaza	Intencional
Amenaza	Personal negligente
Vulnerabilidad	Ausencia de responsabilidades en seguridad de la información en la descripción de los cargos.
Escenario Negativo	El personal realiza el registro de sus operaciones sin seguir los procedimientos indicados en el manual de usuario, cometiendo continuamente los mismos errores, a pesar de ser capacitados en reiteradas ocasiones.

NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.87	2	5	10	**Inaceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					

OPCIONES DE TRATAMIENTO DEL RIESGO			
Aceptar	**Mitigar**	**Compartir**	**Evitar**

Si ha seleccionado mitigar o compartir el riesgo:		
¿Qué salvaguardas aplicaría?		**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**
Salvaguardas Existentes	**Salvaguardas a Implementar**	
- Ninguna.	- Políticas de seguridad de la información. - Responsabilidades y sanciones relacionadas a la seguridad de la información.	Probabilidad

NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.87	2	2	4	**Aceptable**
Reputacional (0.27)	3					
Financiero (0.23)	2					
Legal (0.20)	2					

Tabla 110: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_018]

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_019]					
Riesgo	Habilidades inadecuadas del personal de TI					
Tipo de Amenaza	No intencional					
Amenaza	Personal de TI (programadores)					
Vulnerabilidad	Ausencia de procedimientos para evaluar correctamente las habilidades del personal de TI.					
Escenario Negativo	Se producen fallas durante el uso de las aplicaciones informáticas, debido a que los programadores no implementaron medidas de gestión de excepciones al desarrollar el software.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.60	2	3	6	**Tolerable**
Reputacional (0.27)	2					
Financiero (0.23)	2					
Legal (0.20)	2					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Proceso de selección de personal adecuado.	- Capacitaciones en buenas prácticas de desarrollo de software y otros temas relacionados.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	4	2.60	2	1	2	**Aceptable**
Reputacional (0.27)	2					
Financiero (0.23)	2					
Legal (0.20)	2					

Tabla 111: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_019]

ESCENARIOS DE RIESGO DE LOS PROVEEDORES, TERCEROS Y OUTSOURCING

SELECCIÓN DE OPCIONES DE TRATAMIENTO POR ESCENARIO						
ESCENARIO DE RIESGO						
Código	[ESC_RIE_020]					
Riesgo	Nivel de servicio bajo					
Tipo de Amenaza	Intencional					
Amenaza	Proveedores, outsourcing					
Vulnerabilidad	Ausencia de acuerdos de nivel de servicio (SLAs).					
Escenario Negativo	Se han presentado fallas en el funcionamiento y rendimiento de la infraestructura tecnológica, los cuales no han sido solucionados a tiempo por los proveedores de servicios de TI, generando retrasos en las operaciones de los usuarios.					
NIVEL DE RIESGO INHERENTE						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	**4**	**2.87**	**2**	**5**	**10**	**Inaceptable**
Reputacional (0.27)	**3**					
Financiero (0.23)	**2**					
Legal (0.20)	**2**					
OPCIONES DE TRATAMIENTO DEL RIESGO						
Aceptar	**Mitigar**	**Compartir**	**Evitar**			
Si ha seleccionado mitigar o compartir el riesgo:						
¿Qué salvaguardas aplicaría?					**¿Qué es lo que pretende disminuir: el impacto o la probabilidad?**	
Salvaguardas Existentes	**Salvaguardas a Implementar**					
- Ninguna.	- Acuerdos de nivel de servicio (SLA) adecuados con el proveedor.				Probabilidad	
NIVEL DE RIESGO RESIDUAL						
Área de Impacto	**Valor**	**Impacto Total**	**Impacto (I)**	**Probab. (P)**	**Nivel Riesgo (I * P)**	**Criterio de Aceptación**
Operacional (0.30)	**4**	**2.87**	2	3	6	**Tolerable**
Reputacional (0.27)	**3**					
Financiero (0.23)	**2**					
Legal (0.20)	**2**					

Tabla 112: Selección de Opciones de Tratamiento para el Escenario de Riesgo [ESC_RIE_020]

N°	Escenario de Riesgo		Riesgo Inherente				Tratamiento		Riesgo Residual			
	Código	Riesgo	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación	Opción	Salvaguardas	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación
1	[ESC_RIE_001]	Revelación de datos sensibles	4	3	12	**Inaceptable**	Mitigar	- Cláusulas de confidencialidad en los contratos de trabajo. - Soluciones Data Loss Prevention (DLP).	4	1	4	**Aceptable**
2	[ESC_RIE_002]	Corrupción de datos	2	5	10	**Inaceptable**	Mitigar	- Inducciones cortas brindadas por el área de TI al nuevo personal. - Capacitaciones constantes a todos los usuarios sobre el uso correcto de los aplicativos informáticos. - Desarrollo y actualización periódica de los manuales de usuario.	2	3	6	**Tolerable**
3	[ESC_RIE_003]	Robo de medios de información	3	3	9	**Tolerable**	Mitigar	- Política sobre el uso de dispositivos externos. - Política de escritorio limpio.	3	1	3	**Aceptable**
4	[ESC_RIE_004]	Mal funcionamiento del software	2	5	10	**Inaceptable**	Mitigar	- Metodología de desarrollo de software (gestión de requerimientos). - Procedimientos para la implantación de aplicaciones.	2	2	4	**Aceptable**

N°	Escenario de Riesgo		Riesgo Inherente				Tratamiento		Riesgo Residual			
	Código	Riesgo	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación	Opción	Salvaguardas	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación
5	[ESC_RIE_005]	Abuso de privilegios	2	5	10	**Inaceptable**	Mitigar	- Gestión adecuada de accesos y perfiles de usuario.	2	2	4	**Aceptable**
6	[ESC_RIE_006]	Repudio de transacciones	3	2	6	**Tolerable**	Mitigar	- Tablas y campos de auditoria en la base de datos de los aplicativos informáticos.	3	1	3	**Aceptable**
7	[ESC_RIE_007]	Ataques de Malware	3	3	9	**Tolerable**	Mitigar	- Antivirus. - Configuración de firewall. - Actualizaciones del sistema operativo y aplicaciones. - Filtro antispam. - Copias de seguridad diarias.	1	1	1	**Aceptable**
8	[ESC_RIE_008]	Denegación de acciones	3	2	6	**Tolerable**	Mitigar	- Monitorear las IPs que están accediendo al servidor. - Contratar servicios de proveedor de Internet o hosting web especializados en protección DDoS.	3	1	3	**Aceptable**
9	[ESC_RIE_009]	Phishing / Engaños intencionales	3	4	12	**Inaceptable**	Mitigar	- Antivirus.	3	2	6	**Tolerable**

N°	Escenario de Riesgo		Riesgo Inherente				Tratamiento		Riesgo Residual			
	Código	Riesgo	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación	Opción	Salvaguardas	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación
								- Concientización en cultura de seguridad de la información para el personal. - Plan de seguridad Anti-Phishing.				
10	[ESC_RIE_010]	Incumplimiento con contratos de licencias de software	5	3	15	**Inaceptable**	Mitigar	- Gestión de software instalado en cada computadora. - Adquisición de licencias de software de sistema operativo y paquete ofimático. - Utilizar software libre para las actividades de TI.	5	1	5	**Tolerable**
11	[ESC_RIE_011]	Incumplimiento con reglamentos tributarios	5	2	10	**Inaceptable**	Mitigar	- Funcionalidades de emisión de comprobantes electrónicos en el sistema de la empresa. - Contratar un Operador de Servicios Electrónicos (OSE) para la verificación de sus comprobantes electrónicos.	5	1	5	**Tolerable**
12	[ESC_RIE_012]	Daño a los equipos informáticos	2	5	10	**Inaceptable**	Mitigar	- Mantenimiento correctivo de equipos informáticos.	2	2	4	**Aceptable**

N°	Escenario de Riesgo		Riesgo Inherente				Tratamiento		Riesgo Residual			
	Código	Riesgo	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación	Opción	Salvaguardas	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación
								- Mantenimiento preventivo de equipos informáticos. - Medidas de protección física.				
13	[ESC_RIE_013]	Destrucción de servidores y otros equipos informáticos	4	3	12	**Inaceptable**	Mitigar	- Extintores. - Reubicación del centro de datos.	4	1	4	**Aceptable**
14	[ESC_RIE_014]	Robo de equipos	2	4	8	**Tolerable**	Mitigar	- Cámaras de seguridad en oficinas y otros ambientes. - Políticas de ingreso y salida del personal y otros visitantes.	2	1	2	**Aceptable**
15	[ESC_RIE_015]	Infiltración de agua de lluvia	2	3	6	**Tolerable**	Mitigar	- Acondicionar los ambientes para evitar la infiltración. - Protección física de los equipos.	2	2	4	**Aceptable**
16	[ESC_RIE_016]	Fallas de energía eléctrica	2	5	10	**Inaceptable**	Mitigar	- UPS para los servidores. - Estabilizadores de voltaje. - Equipos UPS para computadoras.	2	2	4	**Aceptable**
17	[ESC_RIE_017]	Desconocimiento del usuario	2	5	10	**Inaceptable**	Mitigar	- Manuales de usuario básicos. - Manuales de usuario por procesos de negocio.	2	2	4	**Aceptable**

N°	Escenario de Riesgo		Riesgo Inherente				Tratamiento		Riesgo Residual			
	Código	Riesgo	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación	Opción	Salvaguardas	Imp. (I)	Prob. (P)	Nivel de Riesgo	Criterio de Aceptación
								- Proceso de inducción adecuado en procesos y aplicativos informáticos.				
18	[ESC_RIE_018]	Negligencia de los usuarios al utilizar los aplicativos informáticos	2	5	10	**Inaceptable**	Mitigar	- Políticas de seguridad de la información. - Responsabilidades y sanciones relacionadas a la seguridad de la información.	2	2	4	**Aceptable**
19	[ESC_RIE_019]	Habilidades inadecuadas del personal de TI	2	3	6	**Tolerable**	Mitigar	- Proceso de selección de personal adecuado. - Capacitaciones en buenas prácticas de desarrollo de software y otros temas relacionados.	2	1	2	**Aceptable**
20	[ESC_RIE_020]	Nivel de servicio bajo	2	5	10	**Inaceptable**	Mitigar	- Acuerdos de nivel de servicio (SLA) adecuados con el proveedor.	2	3	6	**Tolerable**

Tabla 113: Cálculo y Valoración del Riesgo Residual de la Empresa Agroindustrial ABC

10. PASO 10: IMPLEMENTAR LOS PLANES DE TRATAMIENTO DEL RIESGO

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_001]	
2) NOMBRE DEL PROYECTO	
Adquisición de licencias de software de sistema operativo Windows 10 y Microsoft Office 2016	
3) RESPONSABLE	
Nombre	**Cargo**
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
01/07/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_010]	Incumplimiento con contratos de licencias de software
6) JUSTIFICACIÓN	
La empresa requiere la adquisición de 30 licencias software de sistema operativo y paquete ofimático, que permitan al personal realizar sus actividades diarias. De lo contrario, ante cualquier inspección la empresa puede recibir una fuerte multa por parte de INDECOPI, debido al incumplimiento de la Ley sobre el Derecho de Autor. En tal sentido, considerando la necesidad de adquirir las licencias de software de estas herramientas informáticas se realiza el presente proyecto.	
7) ALTERNATIVAS	
Utilización de software libre, como el sistema operativo Ubuntu y Open Office. Ventajas: No se realiza pago alguno por su utilización. No requiere instalación de antivirus. Desventajas: Los usuarios no están muy familiarizados con la utilización de estas herramientas.	
8) ÁREAS BENEFICIARIAS	
Acopio, Calidad, Comercial, Contabilidad, Logística, Producción, Tesorería, Tecnologías de la Información.	
9) CONCLUSIONES	
La adquisición del referido número de licencias de software permitirá realizar las actividades del personal con la legalidad y formalidad solicitada por los entes reguladores.	

Tabla 114: Presentación del Proyecto [PRO_2019_001]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_002]	
2) NOMBRE DEL PROYECTO	
Adquisición de Solución Data Loss Prevention: Endpoint Protector	
3) RESPONSABLE	
Nombre	**Cargo**
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
20/07/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_001]	Revelación de datos sensibles
6) JUSTIFICACIÓN	
La empresa requiere la adquisición de herramientas de prevención de pérdida de datos que aseguren un control granular de puertos USB y periféricos, escanear datos en movimiento y datos en reposo, forzar el cifrado, etc.; de tal manera que se pueda evitar, en lo mayor posible, la filtración de información sensible para la organización. En tal sentido, considerando la necesidad de adquirir estas herramientas informáticas DLP, se realiza el presente proyecto.	
7) ALTERNATIVAS	
Realizar el bloqueo de puertos USB de cada estación de trabajo. Ventajas: No se realiza pago alguno, ya que puede ser realizada por el personal de soporte técnico. Desventajas: No controla la salida de información por otras vías como, por ejemplo: el correo electrónico.	
8) ÁREAS BENEFICIARIAS	
Acopio, Calidad, Comercial, Contabilidad, Logística, Producción, Tesorería, Tecnologías de la Información.	
9) CONCLUSIONES	
La adquisición de una solución DLP permitirá detectar y prevenir el uso y transferencia no autorizada de información confidencial, reforzando así nuestras políticas de seguridad de datos.	

Tabla 115: Presentación del Proyecto [PRO_2019_002]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_003]	
2) NOMBRE DEL PROYECTO	
Capacitaciones a los usuarios sobre el uso correcto de los aplicativos informáticos	
3) RESPONSABLE	
Nombre	**Cargo**
Carlos Rodríguez	Jefe del Área de RRHH
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
22/07/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_002]	Corrupción de datos
[ESC_RIE_017]	Desconocimiento del usuario
6) JUSTIFICACIÓN	
La empresa requiere desarrollar una programación de capacitaciones dirigida a los usuarios, antiguos y nuevos, de las diferentes áreas que hace uso de los aplicativos informáticos. De lo contrario, los usuarios seguirán cometiendo errores al registrar sus operaciones en el sistema, causando daño a la integridad de la información. En tal sentido, considerando la necesidad de evitar la corrupción de la información, se realiza el presente proyecto.	
7) ALTERNATIVAS	
- Ninguna.	
8) ÁREAS BENEFICIARIAS	
Acopio, Calidad, Comercial, Contabilidad, Logística, Producción, Tesorería.	
9) CONCLUSIONES	
La realización de capacitaciones constantes a los usuarios permitirá reducir el número de errores cometidos al registrar sus operaciones en los aplicativos informáticos, evitando así el daño a la información de la empresa.	

Tabla 116: Presentación del Proyecto [PRO_2019_003]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_004]	
2) NOMBRE DEL PROYECTO	
Capacitación e implementación de buenas prácticas en desarrollo de software	
3) RESPONSABLE	
Nombre	**Cargo**
Carlos Rodríguez	Jefe del Área de RRHH
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
09/08/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_004]	Mal funcionamiento del software
[ESC_RIE_019]	Habilidades inadecuadas del personal de TI
6) JUSTIFICACIÓN	
La empresa requiere coordinar con el área de TI capacitaciones que permitan mejorar la calidad del ciclo de vida del desarrollo de los productos software propios de la institución. De lo contrario, seguirán realizándose malas prácticas que perjudiquen el rendimiento de los aplicativos informáticos. En tal sentido, considerando la necesidad de evitar fallas que perjudiquen el rendimiento de los aplicativos informáticos, se realiza el presente proyecto.	
7) ALTERNATIVAS	
Proceso de selección adecuado para personal de TI. Ventajas: No se realiza pago alguno en capacitaciones para el personal de TI, ya que estos vienen con las habilidades adecuadas para el cargo. Desventajas: Con el transcurso del tiempo, estas habilidades pueden volverse obsoletas frente a las nuevas tecnologías emergentes.	
8) ÁREAS BENEFICIARIAS	
Tecnologías de la Información.	
9) CONCLUSIONES	
Las capacitaciones al personal de TI permitirán mejorar la calidad del producto software desarrollado in house, lo que impactará positivamente en el funcionamiento y rendimiento del mismo.	

Tabla 117: Presentación del Proyecto [PRO_2019_004]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_005]	
2) NOMBRE DEL PROYECTO	
Implementación de procedimientos para gestionar adecuadamente los accesos y perfiles de usuario	
3) RESPONSABLE	
Nombre	**Cargo**
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
05/08/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_005]	Abuso de privilegios
6) JUSTIFICACIÓN	
El área de TI requiere implementar procedimientos para administrar correctamente los perfiles y accesos a los usuarios del sistema, agregando o quitando los permisos necesarios. De lo contrario, los usuarios podrían registrar, modificar o eliminar operaciones que no les competen. En tal sentido, considerando la necesidad de implementar procedimientos formales para la revisión de los derechos de acceso de los usuarios, se realiza el presente proyecto.	
7) ALTERNATIVAS	
-Ninguna.	
8) ÁREAS BENEFICIARIAS	
Acopio, Calidad, Comercial, Contabilidad, Logística, Producción, Tesorería.	
9) CONCLUSIONES	
La gestión adecuada de accesos y perfiles permitirá asegurar que estos corresponden a los usuarios correctos, evitando la realización de operaciones no autorizadas.	

Tabla 118: Presentación del Proyecto [PRO_2019_005]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_006]	
2) NOMBRE DEL PROYECTO	
Concientización en cultura de seguridad de la información para el personal	
3) RESPONSABLE	
Nombre	**Cargo**
Carlos Rodríguez	Jefe del Área de RRHH
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
15/08/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_002]	Corrupción de datos
[ESC_RIE_003]	Robo de medios de información
[ESC_RIE_005]	Abuso de privilegios
[ESC_RIE_007]	Ataques de Malware
[ESC_RIE_009]	Phishing / Engaños intencionales
[ESC_RIE_018]	Negligencia de los usuarios al utilizar los aplicativos informáticos
6) JUSTIFICACIÓN	
La empresa requiere organizar capacitaciones o charlas en materia de seguridad de la información, para concientizar al personal sobre la importancia que tiene proteger la información ante cualquier evento o situación de riesgo. De lo contrario, podría volver suceder un incidente como el que se produjo en el año 2017, donde información relevante para la empresa fue pérdida. En tal sentido, considerando la necesidad de concientizar en temas de seguridad de la información al personal de la empresa, se realiza el presente proyecto.	
7) ALTERNATIVAS	
- Ninguna.	
8) ÁREAS BENEFICIARIAS	
Acopio, Calidad, Comercial, Contabilidad, Logística, Producción, Tesorería, Tecnologías de la Información.	
9) CONCLUSIONES	
Las capacitaciones en seguridad de la información permitirán evitar futuros incidentes relacionados con la información como, por ejemplo, ataques phishing, ataques ransomware, entre otros.	

Tabla 119: Presentación del Proyecto [PRO_2019_006]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_007]	
2) NOMBRE DEL PROYECTO	
Contratación de un Operador de Servicios Electrónicos (OSE)	
3) RESPONSABLE	
Nombre	**Cargo**
María Torres	Jefe del Área de Contabilidad
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
01/09/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_011]	Incumplimiento con reglamentos tributarios
6) JUSTIFICACIÓN	
La empresa requiere contratar los servicios de un operador de servicios electrónicos (OSE) para verificar los comprobantes electrónicos emitidos. De lo contrario, la empresa puede incurrir en una falta grave con SUNAT, además que los comprobantes emitidos carecerán de valor legal para deducir gasto y crédito Fiscal. En tal sentido, considerando la necesidad de contratar los servicios de un OSE para poder cumplir con las disposiciones dadas por SUNAT, se realiza el presente proyecto.	
7) ALTERNATIVAS	
- Ninguna.	
8) ÁREAS BENEFICIARIAS	
Contabilidad.	
9) CONCLUSIONES	
Por tratarse de una disposición dada por un ente regulador debe implementarse lo más pronto posible.	

Tabla 120: Presentación del Proyecto [PRO_2019_007]

PRESENTACIÓN DE PROYECTOS PARA EL TRATAMIENTO DEL RIESGO	
1) CÓDIGO	
[PRO_2019_008]	
2) NOMBRE DEL PROYECTO	
Reubicación del centro de datos	
3) RESPONSABLE	
Nombre	**Cargo**
Javier Piscoya	Administrador General
Juan Pérez	Jefe del Área de Tecnologías de la Información
4) FECHA	
21/10/2019	
5) ESCENARIOS DE RIESGO A TRATAR	
Código	**Riesgo**
[ESC_RIE_013]	Destrucción de servidores y otros equipos informáticos
6) JUSTIFICACIÓN	
La empresa requiere reubicar el centro de datos debido a que actualmente se encuentra al costado del taller donde se realiza el mantenimiento de la maquinaria. De lo contrario, al ocurrir algún siniestro en este taller, también podría verse afectado el centro de datos y todos los servidores y equipos informáticos dentro del mismo. En tal sentido, considerando la necesidad de ubicar el centro de datos en un lugar más seguro, se realiza el presente proyecto.	
7) ALTERNATIVAS	
Reubicar el área de mantenimiento.	
8) ÁREAS BENEFICIARIAS	
Tecnologías de la Información.	
9) CONCLUSIONES	
Se debe mantener alejado el centro de datos de áreas susceptibles a un siniestro de incendio.	

Tabla 121: Presentación del Proyecto [PRO_2019_008]

FASE IV: SEGUIMIENTO Y REVISIÓN

11. PASO 11: MONITOREAR LOS ESCENARIOS DE RIESGO

ESCENARIOS DE RIESGO DE LOS DATOS

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_001]	
Riesgo	Revelación de datos sensibles	
Tipo de Amenaza	Intencional	
Amenaza	Ex – Empleados, Personal interno	
Vulnerabilidad	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) de los contratos con el personal.	
Escenario Negativo	Un empleado o ex - empleado filtra información sensible (relacionada a clientes, proveedores, productos, etc.) a los competidores.	
SALVAGUARDAS IMPLEMENTADAS		
- Cláusulas de confidencialidad en los contratos de trabajo. - Soluciones Data Loss Prevention (DLP).		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Competitivo. Interno: Objetivos estratégicos, política interna, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de incidentes de filtración de información sensible.	- Informe de tráfico en la red.	0 filtraciones anuales
- Porcentaje de equipos de cómputo sin protección DLP.	- Inventario de software por equipo.	0%

Tabla 122: Monitorización del Escenario de Riesgo [ESC_RIE_001]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_002]	
Riesgo	Corrupción de datos	
Tipo de Amenaza	No intencional	
Amenaza	Personal no capacitado	
Vulnerabilidad	Configuración incorrecta de parámetros.	
Escenario Negativo	El personal configura de manera errónea los parámetros en la aplicación informática, lo cual ocasiona, que se obtengan y registren datos calculados incorrectamente.	
SALVAGUARDAS IMPLEMENTADAS		
- Inducciones cortas brindadas por el área de TI al nuevo personal. - Capacitaciones constantes a todos los usuarios sobre el uso correcto de los aplicativos informáticos. - Desarrollo y actualización periódica de los manuales de usuario.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Política interna, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de horas de capacitación por usuario.	- Cronograma de capacitaciones.	Más de 2 horas al mes
- Número de tickets registrados por errores de configuración.	- Reporte de tickets registrados.	Menos de 3 tickets al mes

Tabla 123: Monitorización del Escenario de Riesgo [ESC_RIE_002]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_003]	
Riesgo	Robo de medios de información	
Tipo de Amenaza	Intencional	
Amenaza	Personal deshonesto, visitantes, criminales	
Vulnerabilidad	Ausencia de una política sobre limpieza de escritorio y protección de dispositivos de almacenamiento.	
Escenario Negativo	Personas inescrupulosas sustraen documentos impresos y/o dispositivos electrónicos que contienen información importante para la empresa.	
SALVAGUARDAS IMPLEMENTADAS		
- Política sobre el uso de dispositivos externos. - Política de escritorio limpio.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Competitivo. Interno: Objetivos estratégicos, política interna, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de personal que incumple la política de escritorio limpio.	- Informe de supervisión en los puestos de trabajo.	Menos del 5 %
- Número de incidentes de robo de medios de información.	- Reporte de incidentes de robo.	0 incidentes al año

Tabla 124: Monitorización del Escenario de Riesgo [ESC_RIE_003]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_004]	
Riesgo	Mal funcionamiento del software	
Tipo de Amenaza	No intencional	
Amenaza	Personal (desarrolladores)	
Vulnerabilidad	Especificaciones incompletas o no claras para los desarrolladores.	
Escenario Negativo	Los aplicativos informáticos funcionan incorrectamente, debido a que no se hizo un adecuado levantamiento de requerimientos de los usuarios, generando errores y retrasos en los procesos de negocio.	
SALVAGUARDAS IMPLEMENTADAS		
- Metodología de desarrollo de software (gestión de requerimientos). - Procedimientos para la implantación de aplicaciones.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Tecnológico. Interno: Procesos, infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de tickets registrados por fallas del software.	- Reporte de tickets registrados.	Menos de 5 tickets al mes
- Porcentaje de usuarios satisfechos con la calidad del software.	- Encuesta realizada al personal.	Más del 85%

Tabla 125: Monitorización del Escenario de Riesgo [ESC_RIE_004]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_005]	
Riesgo	Abuso de privilegios	
Tipo de Amenaza	Intencional	
Amenaza	Personal malintencionado o negligente	
Vulnerabilidad	Ausencia de un procedimiento formal para la revisión de los derechos de acceso de los usuarios.	
Escenario Negativo	El personal accede indebidamente a los recursos del software ante la presencia de perfiles inadecuados, a través de los cuales, pueden realizar operaciones que no les competen.	
SALVAGUARDAS IMPLEMENTADAS		
- Gestión adecuada de accesos y perfiles de usuario.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Política interna, infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de usuarios con accesos y perfiles inadecuados.	- Reporte de accesos y perfiles de usuario en el sistema.	0%
- Frecuencia de revisiones de accesos y perfiles de usuario en el sistema.	- Informe de actividades del área de TI.	Más de 1 al mes.

Tabla 126: Monitorización del Escenario de Riesgo [ESC_RIE_005]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_006]	
Riesgo	Repudio de transacciones	
Tipo de Amenaza	Intencional	
Amenaza	Personal deshonesto (usuarios del software)	
Vulnerabilidad	Ausencia de pistas de auditoria en los aplicativos informáticos.	
Escenario Negativo	Se han detectado una serie de operaciones fraudulentas en la aplicación informática y no se puede identificar a los responsables.	
SALVAGUARDAS IMPLEMENTADAS		
- Tablas y campos de auditoria en la base de datos de los aplicativos informáticos.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de tablas que no cuentan con pistas de auditoria.	- Reporte de base de datos.	Menos del 5%

Tabla 127: Monitorización del Escenario de Riesgo [ESC_RIE_006]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO	
ESCENARIO DE RIESGO	
Código	[ESC_RIE_007]
Riesgo	Ataques de Malware
Tipo de Amenaza	Intencional
Amenaza	Pirata informático, criminal informático
Vulnerabilidad	Descarga y uso no controlado de software en las estaciones de trabajo.
Escenario Negativo	Se ha producido un ataque de Ransomware, debido a una descarga de software realizada por un usuario, ocasionando la pérdida de archivos importantes.
SALVAGUARDAS IMPLEMENTADAS	
- Antivirus. - Configuración de firewall. - Actualizaciones del sistema operativo y aplicaciones. - Filtro antispam. - Copias de seguridad diarias.	
CONTEXTO EXTERNO E INTERNO INFLUYENTE	
Externo: Tecnológico. Interno: Procesos, infraestructura tecnológica, cultura organizacional.	
MÉTRICAS DE EVALUACIÓN	

Métrica	Fuente de Información	Valor
- Porcentaje de computadoras sin protección antivirus.	- Inventario de software por equipo.	0%
- Frecuencia de generación de copias de seguridad de archivos de los usuarios.	- Informe de actividades del área de TI.	1 al día

Tabla 128: Monitorización del Escenario de Riesgo [ESC_RIE_007]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_008]	
Riesgo	Denegación de acciones	
Tipo de Amenaza	Intencional	
Amenaza	Pirata informático	
Vulnerabilidad	Deficiente configuración Routers y Firewalls.	
Escenario Negativo	Se ha producido un ataque distribuido de denegación de servicios (DDoS), que ha provocado la caída de la red e imposibilita el acceso a los aplicativos informáticos.	
SALVAGUARDAS IMPLEMENTADAS		
- Monitorear las IPs que están accediendo al servidor. - Contratar servicios de proveedor de Internet o hosting web especializados en protección DDoS.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Competitivo, tecnológico. Interno: Procesos, infraestructura tecnológica.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de ancho de banda a internet consumido.	- Informe de tráfico en la red.	Menos del 70%
- Número de interrupciones de negocio debidas a incidentes de caída de la red.	- Reporte de tickets registrados.	Menos de 5 al año

Tabla 129: Monitorización del Escenario de Riesgo [ESC_RIE_008]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO			
ESCENARIO DE RIESGO			
Código	[ESC_RIE_009]		
Riesgo	Phishing / Engaños intencionales		
Tipo de Amenaza	Intencional		
Amenaza	Criminal informático, espionaje industrial (otras empresas).		
Vulnerabilidad	Falta de conciencia acerca de la seguridad de la información del personal.		
Escenario Negativo	El personal ha sido víctima de un ataque de Phishing, a través del cual, se ha visto comprometida información sensible de la empresa.		
SALVAGUARDAS IMPLEMENTADAS			
- Antivirus. - Concientización en cultura de seguridad de la información para el personal. - Plan de seguridad Anti-Phishing.			
CONTEXTO EXTERNO E INTERNO INFLUYENTE			
Externo: Competitivo. Interno: Política interna, procesos, cultura organizacional.			
MÉTRICAS DE EVALUACIÓN			
Métrica		**Fuente de Información**	**Valor**
- Porcentaje de computadoras sin protección antivirus.		- Inventario de software por equipo.	0%
- Frecuencia de capacitaciones en temas de seguridad informática al personal.		- Cronograma de capacitaciones.	Al menos 1 al mes

Tabla 130: Monitorización del Escenario de Riesgo [ESC_RIE_009]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_010]	
Riesgo	Incumplimiento con contratos de licencias de software	
Tipo de Amenaza	Intencional	
Amenaza	Entidades reguladoras	
Vulnerabilidad	El número de instalaciones de un software propietario sobrepasa el número de licencias adquiridas.	
Escenario Negativo	La empresa ha recibido una multa de INDECOPI, debido a la presencia de software propietario instalado sin licencia o que sobrepasa el número instalaciones permitidas.	
SALVAGUARDAS IMPLEMENTADAS		
- Gestión de software instalado en cada computadora. - Adquisición de licencias de software de sistema operativo y paquete ofimático. - Utilizar software libre para las actividades de TI.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Político, Legal y regulatorio, tecnológico, proveedores. Interno: Procesos, política interna, infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de computadoras con software instalado sin licencia.	- Inventario de software por equipo.	Menos del 5%
- Número de incumplimientos de TI reportados a la Alta Dirección.	- Informe de auditoría de sistemas.	Menos de 3

Tabla 131: Monitorización del Escenario de Riesgo [ESC_RIE_010]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_011]	
Riesgo	Incumplimiento con reglamentos tributarios	
Tipo de Amenaza	Intencional	
Amenaza	Entidades reguladoras	
Vulnerabilidad	Ausencia de un módulo o aplicación contable que emita comprobantes electrónicos.	
Escenario Negativo	La empresa es sancionada por SUNAT al incumplir con la emisión de comprobantes electrónicos, debido a que su aplicación informática no cuenta con dicha funcionalidad.	
SALVAGUARDAS IMPLEMENTADAS		
- Funcionalidades de emisión de comprobantes electrónicos en el sistema de la empresa. - Contratar un Operador de Servicios Electrónicos (OSE) para la verificación de sus comprobantes electrónicos.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Político, legal y regulatorio, tecnológico, proveedores. Interno: Procesos, infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Coste de incumplimientos de TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación.	- Informe de multas.	Menos de S/ 5,000
- Número de incumplimientos de TI reportados a la Alta Dirección o causantes de comentarios o vergüenza pública.	- Informe de auditoría de sistemas.	Menos de 3

Tabla 132: Monitorización del Escenario de Riesgo [ESC_RIE_011]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_012]	
Riesgo	Daño a los equipos informáticos	
Tipo de Amenaza	Naturales	
Amenaza	Polvo, corrosión, humedad	
Vulnerabilidad	Susceptibilidad al polvo, corrosión y humedad.	
Escenario Negativo	Los equipos informáticos de la empresa se ven dañados debido a que no se han implementado las medidas de protección físicas adecuadas.	
SALVAGUARDAS IMPLEMENTADAS		
- Mantenimiento correctivo de equipos informáticos. - Mantenimiento preventivo de equipos informáticos. - Medidas de protección física.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Medioambiental. Interno: Procesos, infraestructura tecnológica.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Frecuencia de mantenimientos preventivos a los equipos informáticos.	- Informes de mantenimiento.	Al menos 1 al mes
- Porcentaje de equipos informáticos sin medidas de protección físicas.	- Inventario de equipos.	Menos del 10%

Tabla 133: Monitorización del Escenario de Riesgo [ESC_RIE_012]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_013]	
Riesgo	Destrucción de servidores y otros equipos informáticos	
Tipo de Amenaza	No intencional	
Amenaza	Incendio	
Vulnerabilidad	Ubicación en área susceptible de incendios.	
Escenario Negativo	Se produce un incendio en el taller de mantenimiento, el cual está ubicado al costado del área donde se encuentran los servidores de la empresa. Como consecuencia de esto, los servidores y otros equipos informáticos fueron destruidos.	
SALVAGUARDAS IMPLEMENTADAS		
- Extintores. - Reubicación del centro de datos.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Procesos, infraestructura tecnológica.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de siniestros donde se ven comprometidos equipos informáticos.	- Informe de siniestros ocurridos.	Menos de 3 al año
- Número de incumplimientos de estándares internacionales con respecto al Data Center.	- Informe de auditoría de sistemas.	Menos de 5

Tabla 134: Monitorización del Escenario de Riesgo [ESC_RIE_013]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_014]	
Riesgo	Robo de equipos	
Tipo de Amenaza	Intencional	
Amenaza	Personal deshonesto, visitantes	
Vulnerabilidad	Ausencia de protección física de la edificación (paredes, puertas y ventanas) y dispositivos de videovigilancia.	
Escenario Negativo	Se han extraído ilícitamente equipos informáticos de las instalaciones de la empresa. Además, los implicados no pueden ser identificados debido a la ausencia de registros en videos.	
SALVAGUARDAS IMPLEMENTADAS		
- Cámaras de seguridad en oficinas y otros ambientes. - Políticas de ingreso y salida del personal y otros visitantes.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Política interna, infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de incidentes de equipos sustraídos ilícitamente.	- Reporte de equipos robados.	0
- Porcentaje de ambientes sin medidas de videovigilancia implementadas.	- Informe de cámaras de seguridad.	Menos del 20%

Tabla 135: Monitorización del Escenario de Riesgo [ESC_RIE_014]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_015]	
Riesgo	Infiltración de agua de lluvia	
Tipo de Amenaza	Naturales	
Amenaza	Fenómeno de "El Niño"	
Vulnerabilidad	Ubicación de instalaciones en áreas susceptibles de inundación.	
Escenario Negativo	Se han presentado intensas lluvias que han afectado a varios componentes físicos del sistema de información, debido a que los ambientes donde se encontraban alojados presentaban deficiencias por donde se infiltró el agua de lluvia.	
SALVAGUARDAS IMPLEMENTADAS		
- Acondicionar los ambientes para evitar la infiltración. - Protección física de los equipos.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Medioambiental. Interno: Procesos, infraestructura tecnológica, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de ambientes propensos a infiltración de agua de lluvia.	- Informe de estado de la infraestructura.	Menos del 15%
- Porcentaje de equipos informáticos sin medidas de protección físicas.	- Inventario de equipos.	Menos del 10%

Tabla 136: Monitorización del Escenario de Riesgo [ESC_RIE_015]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_016]	
Riesgo	Fallas de energía eléctrica	
Tipo de Amenaza	No intencional	
Amenaza	Red energética inestable	
Vulnerabilidad	Susceptibilidad de los equipos informáticos a las variaciones de voltaje.	
Escenario Negativo	El suministro eléctrico presenta variaciones de voltaje que afectan a los equipos informáticos, causando interrupciones en las operaciones diarias de la empresa.	
SALVAGUARDAS IMPLEMENTADAS		
- UPS para los servidores. - Estabilizadores de voltaje. - Equipos UPS para computadoras.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Procesos, infraestructura tecnológica.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de interrupciones de negocio debidas a incidentes de energía eléctrica.	- Reporte de tickets registrados.	No más de 1 al mes.
- Porcentaje de computadoras con UPS.	- Inventario de equipos.	Al menos el 75%

Tabla 137: Monitorización del Escenario de Riesgo [ESC_RIE_016]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_017]	
Riesgo	Desconocimiento del usuario	
Tipo de Amenaza	No intencional	
Amenaza	Personal no capacitado	
Vulnerabilidad	Ausencia de procedimientos de inducción al personal en el uso de los aplicativos informáticos.	
Escenario Negativo	Los usuarios del sistema cometen errores al realizar el registro de sus operaciones, afectando a la información del negocio y causando errores de otras áreas que hacen uso de esta información.	
SALVAGUARDAS IMPLEMENTADAS		
- Manuales de usuario básicos. - Manuales de usuario por procesos de negocio. - Proceso de inducción adecuado en procesos y aplicativos informáticos.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Objetivos estratégicos, política interna, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Nivel de satisfacción de los usuarios de negocio con la formación y los manuales de usuario.	- Encuesta realizada al personal.	Al menos 7 de NPS
- Número de horas de formación al personal nuevo en procesos y aplicativos informáticos	- Cronograma de capacitaciones.	Al menos 24 horas

Tabla 138: Monitorización del Escenario de Riesgo [ESC_RIE_017]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_018]	
Riesgo	Negligencia de los usuarios al utilizar los aplicativos informáticos	
Tipo de Amenaza	Intencional	
Amenaza	Personal negligente	
Vulnerabilidad	Ausencia de responsabilidades en seguridad de la información en la descripción de los cargos.	
Escenario Negativo	El personal realiza el registro de sus operaciones sin seguir los procedimientos indicados en el manual de usuario, cometiendo continuamente los mismos errores, a pesar de ser capacitados en reiteradas ocasiones.	
SALVAGUARDAS IMPLEMENTADAS		
- Políticas de seguridad de la información. - Responsabilidades y sanciones relacionadas a la seguridad de la información.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Interno: Procesos, política interna, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de incidentes relacionados con el incumplimiento de políticas seguridad de la información.	- Reporte de tickets registrados.	No más de 10 al mes
- Porcentaje de usuarios que cometen errores constantemente.	- Reporte de tickets registrados.	No más del 5%

Tabla 139: Monitorización del Escenario de Riesgo [ESC_RIE_018]

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_019]	
Riesgo	Habilidades inadecuadas del personal de TI	
Tipo de Amenaza	No intencional	
Amenaza	Personal de TI (programadores)	
Vulnerabilidad	Ausencia de procedimientos para evaluar correctamente las habilidades del personal de TI.	
Escenario Negativo	Se producen fallas durante el uso de las aplicaciones informáticas, debido a que los programadores no implementaron medidas de gestión de excepciones al desarrollar el software.	
SALVAGUARDAS IMPLEMENTADAS		
- Proceso de selección de personal adecuado. - Capacitaciones en buenas prácticas de desarrollo de software y otros temas relacionados.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Tecnológico. Interno: Objetivos estratégicos, política interna, procesos, cultura organizacional.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles.	- Evaluación al personal.	Más del 85%
- Número de incidentes del procesamiento de negocio causados por errores del personal de TI.	- Reporte de tickets registrados.	No más de 3 al mes

Tabla 140: Monitorización del Escenario de Riesgo [ESC_RIE_019]

ESCENARIOS DE RIESGO DE LOS PROVEEDORES, TERCEROS Y OUTSOURCING

MONITORIZACIÓN DEL ESCENARIO DE RIESGO		
ESCENARIO DE RIESGO		
Código	[ESC_RIE_020]	
Riesgo	Nivel de servicio bajo	
Tipo de Amenaza	Intencional	
Amenaza	Proveedores, outsourcing	
Vulnerabilidad	Ausencia de acuerdos de nivel de servicio (SLAs).	
Escenario Negativo	Se han presentado fallas en el funcionamiento y rendimiento de la infraestructura tecnológica, los cuales no han sido solucionados a tiempo por los proveedores de servicios de TI, generando retrasos en las operaciones de los usuarios.	
SALVAGUARDAS IMPLEMENTADAS		
- Acuerdos de nivel de servicio (SLA) adecuados con el proveedor.		
CONTEXTO EXTERNO E INTERNO INFLUYENTE		
Externo: Proveedores. Interno: Política interna, procesos, infraestructura tecnológica.		
MÉTRICAS DE EVALUACIÓN		
Métrica	**Fuente de Información**	**Valor**
- Número de incumplimientos relacionados con proveedores de servicios de TI.	- Reporte de tickets registrados.	Menos de 5 al año
- Número de horas que un proceso critico se ve interrumpido.	- RTO de cada proceso crítico.	No debe superar el RTO de cada proceso crítico

Tabla 141: Monitorización del Escenario de Riesgo [ESC_RIE_020]

ANEXO 5: MATRIZ DE CONSISTENCIA DE VALIDACIÓN DE EXPERTOS

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

Objetivo: La matriz de consistencia tiene como objetivo contrastar la validez del modelo de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario, a partir de la investigación de las distintas metodologías y estándares de gestión de riesgos de TI, un modelo simplificado y flexible que promueva su aplicación, con la intención de que se desarrolle una cultura organizacional de acción preventiva en la gestión de riesgos de tecnologías de la información en las empresas del sector agroindustrial.

Escala de calificación: (1) Totalmente en desacuerdo (2) En desacuerdo (3) Neutral (4) De acuerdo (5) Totalmente de acuerdo

Instrucciones: Por favor marcar con (X) según la opción elegida.

FASE I: DEFINICIÓN DEL ALCANCE, CONTEXTO Y CRITERIOS								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 01: Identificar los Procesos Críticos, Áreas Involucradas y Activos	Identificar los procesos de negocio críticos de la empresa.	Nivel de adecuación con respecto a la selección de procesos críticos de empresas agroindustriales.				X		
	Identificar las áreas de negocio relevantes para el proceso de gestión del riesgo.	Nivel de simplicidad para identificar las áreas de negocio que gestionan los procesos críticos.				X		
	Identificar los activos que deben ser incluidos en el proceso de gestión del riesgo.	Nivel de practicidad para identificar los activos que intervienen en los procesos críticos.				X		
Paso 02: Identificar el Contexto Externo e Interno	Conocer los factores externos que pueden influir sobre los escenarios de riesgo.	Nivel de pertinencia de los factores externos seleccionados.				X		
	Conocer los factores internos que pueden	Nivel de pertinencia de los factores internos seleccionados.				X		

	influir sobre los escenarios de riesgo.							
Paso 03: Identificar las Áreas de Impacto del Riesgo	Identificar y ponderar los tipos de impacto que puede sufrir la empresa.	Nivel de pertinencia de las áreas de impacto seleccionadas.					X	
		Nivel de simplicidad para ponderar las áreas de impacto del riesgo.						
Paso 04: Definir Escalas de Valoración del Impacto y la Probabilidad del Riesgo	Definir escalas de valoración para cada área de impacto del riesgo.	Número de escalas suficientes para valorar las áreas de impacto del riesgo.					X	
	Definir la fórmula de cálculo y escalas de valoración del impacto total del riesgo.	Nivel de suficiencia de la fórmula para calcular el impacto total del riesgo.					X	
		Número de escalas suficientes para valorar el impacto total del riesgo.						
	Definir escalas de valoración de la probabilidad del riesgo.	Número de escalas suficientes para medir la probabilidad de ocurrencia del riesgo.					X	
Paso 05: Definir Criterios de Aceptación del Riesgo	Establecer los niveles de riesgo que la empresa está dispuesta a aceptar para alcanzar sus objetivos.	Número de niveles obtenidos en el mapa de calor del riesgo propuesto.					X	
		Nivel de suficiencia de las escalas de aceptación del riesgo (aceptable, tolerable, inaceptable) y rangos propuestos.				X		

FASE II: EVALUACIÓN DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 06: Elaborar Escenarios de Riesgo	Conocer y describir situaciones de riesgo dentro de la empresa.	Nivel de simplicidad para caracterizar escenarios de riesgo, de acuerdo a los ítems definidos.					X	
Paso 07: Calcular y Valorar el Riesgo Inherente	Conocer el nivel de riesgo de cada escenario, antes de aplicar cualquier control o salvaguarda.	Nivel de practicidad para calcular el riesgo inherente de cada escenario, según la valoración de impacto y probabilidad asignados.					X	
	Valorar el riesgo inherente de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo inherente, según los criterios de aceptación definidos por la empresa.					X	
FASE III: TRATAMIENTO DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 08: Definir Opciones de Tratamiento del Riesgo	Conocer las opciones de tratamiento más convenientes para hacer frente a los escenarios de riesgo.	Nivel de suficiencia con respecto a la definición de las opciones de tratamiento del riesgo (Aceptar, Mitigar, Compartir, Evitar).				X		
Paso 09: Calcular y Valorar el Riesgo Residual	Conocer el nivel de riesgo de cada escenario, después de aplicar la opción de tratamiento más adecuada.	Nivel de practicidad para calcular el riesgo residual de cada escenario, según la valoración de impacto y probabilidad resultantes.					X	
	Valorar el riesgo residual de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo residual, según los criterios de aceptación definidos por la empresa.				X		

Paso 10: Implementar los Planes de Tratamiento del Riesgo	Formular proyectos para poner en marcha las opciones de tratamiento que han sido seleccionadas.	Nivel de simplicidad para la formulación de proyectos que implementen los controles o salvaguardas.				X		
FASE IV: SEGUIMIENTO Y REVISIÓN								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 11: Monitorear los Escenarios de Riesgo	Identificar el contexto influyente que debe ser supervisado.	Nivel de simplicidad para definir el contexto externo e interno que debe ser monitoreado.				X		
	Identificar métricas que permitan supervisar cada escenario de riesgo.	Nivel de practicidad para monitorear cada escenario de riesgo, según las métricas definidas.				X		

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	✓

DR. ERNESTO KARLO CELI ARÉVALO

PROFESIONAL EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

Objetivo: La matriz de consistencia tiene como objetivo contrastar la validez del modelo de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario, a partir de la investigación de las distintas metodologías y estándares de gestión de riesgos de TI, un modelo simplificado y flexible que promueva su aplicación, con la intención de que se desarrolle una cultura organizacional de acción preventiva en la gestión de riesgos de tecnologías de la información en las empresas del sector agroindustrial.

Escala de calificación: (1) Totalmente en desacuerdo (2) En desacuerdo (3) Neutral (4) De acuerdo (5) Totalmente de acuerdo

Instrucciones: Por favor marcar con (X) según la opción elegida.

FASE I: DEFINICIÓN DEL ALCANCE, CONTEXTO Y CRITERIOS								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 01: Identificar los Procesos Críticos, Áreas Involucradas y Activos	Identificar los procesos de negocio críticos de la empresa.	Nivel de adecuación con respecto a la selección de procesos críticos de empresas agroindustriales.					X	
	Identificar las áreas de negocio relevantes para el proceso de gestión del riesgo.	Nivel de simplicidad para identificar las áreas de negocio que gestionan los procesos críticos.					X	
	Identificar los activos que deben ser incluidos en el proceso de gestión del riesgo.	Nivel de practicidad para identificar los activos que intervienen en los procesos críticos.				X		Diferenciar mobiliario, preferible especificar lo prioritario como gabinetes o racks
Paso 02: Identificar el Contexto Externo e Interno	Conocer los factores externos que pueden influir sobre los escenarios de riesgo.	Nivel de pertinencia de los factores externos seleccionados.					X	
	Conocer los factores internos que pueden	Nivel de pertinencia de los factores internos seleccionados.					X	

	influir sobre los escenarios de riesgo.							
Paso 03: Identificar las Áreas de Impacto del Riesgo	Identificar y ponderar los tipos de impacto que puede sufrir la empresa.	Nivel de pertinencia de las áreas de impacto seleccionadas.					X	
		Nivel de simplicidad para ponderar las áreas de impacto del riesgo.					X	
Paso 04: Definir Escalas de Valoración del Impacto y la Probabilidad del Riesgo	Definir escalas de valoración para cada área de impacto del riesgo.	Número de escalas suficientes para valorar las áreas de impacto del riesgo.					X	
	Definir la fórmula de cálculo y escalas de valoración del impacto total del riesgo.	Nivel de suficiencia de la fórmula para calcular el impacto total del riesgo.					X	
		Número de escalas suficientes para valorar el impacto total del riesgo.					X	
	Definir escalas de valoración de la probabilidad del riesgo.	Número de escalas suficientes para medir la probabilidad de ocurrencia del riesgo.					X	
Paso 05: Definir Criterios de Aceptación del Riesgo	Establecer los niveles de riesgo que la empresa está dispuesta a aceptar para alcanzar sus objetivos.	Número de niveles obtenidos en el mapa de calor del riesgo propuesto.					X	
		Nivel de suficiencia de las escalas de aceptación del riesgo (aceptable, tolerable, inaceptable) y rangos propuestos.					X	

FASE II: EVALUACIÓN DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 06: Elaborar Escenarios de Riesgo	Conocer y describir situaciones de riesgo dentro de la empresa.	Nivel de simplicidad para caracterizar escenarios de riesgo, de acuerdo a los ítems definidos.				X		Especificar código de los procesos.
Paso 07: Calcular y Valorar el Riesgo Inherente	Conocer el nivel de riesgo de cada escenario, antes de aplicar cualquier control o salvaguarda.	Nivel de practicidad para calcular el riesgo inherente de cada escenario, según la valoración de impacto y probabilidad asignados.					X	
	Valorar el riesgo inherente de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo inherente, según los criterios de aceptación definidos por la empresa.					X	
FASE III: TRATAMIENTO DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 08: Definir Opciones de Tratamiento del Riesgo	Conocer las opciones de tratamiento más convenientes para hacer frente a los escenarios de riesgo.	Nivel de suficiencia con respecto a la definición de las opciones de tratamiento del riesgo (Aceptar, Mitigar, Compartir, Evitar).					X	
Paso 09: Calcular y Valorar el Riesgo Residual	Conocer el nivel de riesgo de cada escenario, después de aplicar la opción de tratamiento más adecuada.	Nivel de practicidad para calcular el riesgo residual de cada escenario, según la valoración de impacto y probabilidad resultantes.					X	
	Valorar el riesgo residual de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo residual, según los criterios de aceptación definidos por la empresa.					X	

Paso 10: Implementar los Planes de Tratamiento del Riesgo	Formular proyectos para poner en marcha las opciones de tratamiento que han sido seleccionadas.	Nivel de simplicidad para la formulación de proyectos que implementen los controles o salvaguardas.					X	
FASE IV: SEGUIMIENTO Y REVISIÓN								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 11: Monitorear los Escenarios de Riesgo	Identificar el contexto influyente que debe ser supervisado.	Nivel de simplicidad para definir el contexto externo e interno que debe ser monitoreado.					X	
	Identificar métricas que permitan supervisar cada escenario de riesgo.	Nivel de practicidad para monitorear cada escenario de riesgo, según las métricas definidas.					X	

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	✓

DRA. JESSIE LEILA BRAVO JAICO

PROFESIONAL EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

Objetivo: La matriz de consistencia tiene como objetivo contrastar la validez del modelo de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario, a partir de la investigación de las distintas metodologías y estándares de gestión de riesgos de TI, un modelo simplificado y flexible que promueva su aplicación, con la intención de que se desarrolle una cultura organizacional de acción preventiva en la gestión de riesgos de tecnologías de la información en las empresas del sector agroindustrial.

Escala de calificación: (1) Totalmente en desacuerdo (2) En desacuerdo (3) Neutral (4) De acuerdo (5) Totalmente de acuerdo

Instrucciones: Por favor marcar con (X) según la opción elegida.

FASE I: DEFINICIÓN DEL ALCANCE, CONTEXTO Y CRITERIOS								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 01: Identificar los Procesos Críticos, Áreas Involucradas y Activos	Identificar los procesos de negocio críticos de la empresa.	Nivel de adecuación con respecto a la selección de procesos críticos de empresas agroindustriales.					X	
	Identificar las áreas de negocio relevantes para el proceso de gestión del riesgo.	Nivel de simplicidad para identificar las áreas de negocio que gestionan los procesos críticos.				X		
	Identificar los activos que deben ser incluidos en el proceso de gestión del riesgo.	Nivel de practicidad para identificar los activos que intervienen en los procesos críticos.				X		
Paso 02: Identificar el Contexto Externo e Interno	Conocer los factores externos que pueden influir sobre los escenarios de riesgo.	Nivel de pertinencia de los factores externos seleccionados.					X	
	Conocer los factores internos que pueden	Nivel de pertinencia de los factores internos seleccionados.				X		

	influir sobre los escenarios de riesgo.							
Paso 03: Identificar las Áreas de Impacto del Riesgo	Identificar y ponderar los tipos de impacto que puede sufrir la empresa.	Nivel de pertinencia de las áreas de impacto seleccionadas.				X		
		Nivel de simplicidad para ponderar las áreas de impacto del riesgo.				X		
Paso 04: Definir Escalas de Valoración del Impacto y la Probabilidad del Riesgo	Definir escalas de valoración para cada área de impacto del riesgo.	Número de escalas suficientes para valorar las áreas de impacto del riesgo.				X		
	Definir la fórmula de cálculo y escalas de valoración del impacto total del riesgo.	Nivel de suficiencia de la fórmula para calcular el impacto total del riesgo.				X		
		Número de escalas suficientes para valorar el impacto total del riesgo.				X		
	Definir escalas de valoración de la probabilidad del riesgo.	Número de escalas suficientes para medir la probabilidad de ocurrencia del riesgo.				X		
Paso 05: Definir Criterios de Aceptación del Riesgo	Establecer los niveles de riesgo que la empresa está dispuesta a aceptar para alcanzar sus objetivos.	Número de niveles obtenidos en el mapa de calor del riesgo propuesto.					X	
		Nivel de suficiencia de las escalas de aceptación del riesgo (aceptable, tolerable, inaceptable) y rangos propuestos.					X	

FASE II: EVALUACIÓN DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 06: Elaborar Escenarios de Riesgo	Conocer y describir situaciones de riesgo dentro de la empresa.	Nivel de simplicidad para caracterizar escenarios de riesgo, de acuerdo a los ítems definidos.					X	
Paso 07: Calcular y Valorar el Riesgo Inherente	Conocer el nivel de riesgo de cada escenario, antes de aplicar cualquier control o salvaguarda.	Nivel de practicidad para calcular el riesgo inherente de cada escenario, según la valoración de impacto y probabilidad asignados.					X	
	Valorar el riesgo inherente de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo inherente, según los criterios de aceptación definidos por la empresa.					X	
FASE III: TRATAMIENTO DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 08: Definir Opciones de Tratamiento del Riesgo	Conocer las opciones de tratamiento más convenientes para hacer frente a los escenarios de riesgo.	Nivel de suficiencia con respecto a la definición de las opciones de tratamiento del riesgo (Aceptar, Mitigar, Compartir, Evitar).				X		
Paso 09: Calcular y Valorar el Riesgo Residual	Conocer el nivel de riesgo de cada escenario, después de aplicar la opción de tratamiento más adecuada.	Nivel de practicidad para calcular el riesgo residual de cada escenario, según la valoración de impacto y probabilidad resultantes.					X	
	Valorar el riesgo residual de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo residual, según los criterios de aceptación definidos por la empresa.					X	

Paso 10: Implementar los Planes de Tratamiento del Riesgo	Formular proyectos para poner en marcha las opciones de tratamiento que han sido seleccionadas.	Nivel de simplicidad para la formulación de proyectos que implementen los controles o salvaguardas.				X		
FASE IV: SEGUIMIENTO Y REVISIÓN								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 11: Monitorear los Escenarios de Riesgo	Identificar el contexto influyente que debe ser supervisado.	Nivel de simplicidad para definir el contexto externo e interno que debe ser monitoreado.					X	
	Identificar métricas que permitan supervisar cada escenario de riesgo.	Nivel de practicidad para monitorear cada escenario de riesgo, según las métricas definidas.					X	

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	X

DR. GILBERTO CARRIÓN BARCO

PROFESIONAL EXPERTO

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

Objetivo: La matriz de consistencia tiene como objetivo contrastar la validez del modelo de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque. El modelo propuesto se enfoca en brindar al usuario, a partir de la investigación de las distintas metodologías y estándares de gestión de riesgos de TI, un modelo simplificado y flexible que promueva su aplicación, con la intención de que se desarrolle una cultura organizacional de acción preventiva en la gestión de riesgos de tecnologías de la información en las empresas del sector agroindustrial.

Escala de calificación: (1) Totalmente en desacuerdo (2) En desacuerdo (3) Neutral (4) De acuerdo (5) Totalmente de acuerdo

Instrucciones: Por favor marcar con (X) según la opción elegida.

FASE I: DEFINICIÓN DEL ALCANCE, CONTEXTO Y CRITERIOS								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 01: Identificar los Procesos Críticos, Áreas Involucradas y Activos	Identificar los procesos de negocio críticos de la empresa.	Nivel de adecuación con respecto a la selección de procesos críticos de empresas agroindustriales.					X	
	Identificar las áreas de negocio relevantes para el proceso de gestión del riesgo.	Nivel de simplicidad para identificar las áreas de negocio que gestionan los procesos críticos.					X	
	Identificar los activos que deben ser incluidos en el proceso de gestión del riesgo.	Nivel de practicidad para identificar los activos que intervienen en los procesos críticos.					X	
Paso 02: Identificar el Contexto Externo e Interno	Conocer los factores externos que pueden influir sobre los escenarios de riesgo.	Nivel de pertinencia de los factores externos seleccionados.				X		
	Conocer los factores internos que pueden	Nivel de pertinencia de los factores internos seleccionados.				X		

	influir sobre los escenarios de riesgo.								
Paso 03: Identificar las Áreas de Impacto del Riesgo	Identificar y ponderar los tipos de impacto que puede sufrir la empresa.	Nivel de pertinencia de las áreas de impacto seleccionadas.				X			
		Nivel de simplicidad para ponderar las áreas de impacto del riesgo.				X			
Paso 04: Definir Escalas de Valoración del Impacto y la Probabilidad del Riesgo	Definir escalas de valoración para cada área de impacto del riesgo.	Número de escalas suficientes para valorar las áreas de impacto del riesgo.					X		
	Definir la fórmula de cálculo y escalas de valoración del impacto total del riesgo.	Nivel de suficiencia de la fórmula para calcular el impacto total del riesgo.					X		
		Número de escalas suficientes para valorar el impacto total del riesgo.					X		
	Definir escalas de valoración de la probabilidad del riesgo.	Número de escalas suficientes para medir la probabilidad de ocurrencia del riesgo.				X			
Paso 05: Definir Criterios de Aceptación del Riesgo	Establecer los niveles de riesgo que la empresa está dispuesta a aceptar para alcanzar sus objetivos.	Número de niveles obtenidos en el mapa de calor del riesgo propuesto.				X			
		Nivel de suficiencia de las escalas de aceptación del riesgo (aceptable, tolerable, inaceptable) y rangos propuestos.				X			

FASE II: EVALUACIÓN DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 06: Elaborar Escenarios de Riesgo	Conocer y describir situaciones de riesgo dentro de la empresa.	Nivel de simplicidad para caracterizar escenarios de riesgo, de acuerdo a los ítems definidos.				X		
Paso 07: Calcular y Valorar el Riesgo Inherente	Conocer el nivel de riesgo de cada escenario, antes de aplicar cualquier control o salvaguarda.	Nivel de practicidad para calcular el riesgo inherente de cada escenario, según la valoración de impacto y probabilidad asignados.				X		
	Valorar el riesgo inherente de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo inherente, según los criterios de aceptación definidos por la empresa.					X	
FASE III: TRATAMIENTO DEL RIESGO								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 08: Definir Opciones de Tratamiento del Riesgo	Conocer las opciones de tratamiento más convenientes para hacer frente a los escenarios de riesgo.	Nivel de suficiencia con respecto a la definición de las opciones de tratamiento del riesgo (Aceptar, Mitigar, Compartir, Evitar).					X	
Paso 09: Calcular y Valorar el Riesgo Residual	Conocer el nivel de riesgo de cada escenario, después de aplicar la opción de tratamiento más adecuada.	Nivel de practicidad para calcular el riesgo residual de cada escenario, según la valoración de impacto y probabilidad resultantes.				X		
	Valorar el riesgo residual de cada escenario, según los criterios de aceptación.	Nivel de simplicidad para valorar el riesgo residual, según los criterios de aceptación definidos por la empresa.				X		

Paso 10: Implementar los Planes de Tratamiento del Riesgo	Formular proyectos para poner en marcha las opciones de tratamiento que han sido seleccionadas.	Nivel de simplicidad para la formulación de proyectos que implementen los controles o salvaguardas.				X		
FASE IV: SEGUIMIENTO Y REVISIÓN								
Paso	**Objetivo**	**Descripción del Indicador**	**1**	**2**	**3**	**4**	**5**	**Observaciones**
Paso 11: Monitorear los Escenarios de Riesgo	Identificar el contexto influyente que debe ser supervisado.	Nivel de simplicidad para definir el contexto externo e interno que debe ser monitoreado.				X		
	Identificar métricas que permitan supervisar cada escenario de riesgo.	Nivel de practicidad para monitorear cada escenario de riesgo, según las métricas definidas.				X		

DISCONFORMIDAD	
OBSERVADO	
ACEPTACIÓN	X

MGTR. HOBBER ARISTIDES SICCHA AYVAR

PROFESIONAL EXPERTO

ANEXO 6: PERFIL DE LOS PROFESIONALES EXPERTOS

ERNESTO KARLO CELI ARÉVALO

Gestión de la Seguridad de Información, Riesgos TI y Continuidad de Procesos

PERFIL

Especialista en Seguridad y Auditoría Informática con COSO, COBIT 5.0, ISO/IEC 27001, ISO/IEC 27002. Especialista en Gestión de Riesgos de TI con ISO/IEC 27005, Magerit. Especialista en Gestión de servicios de TI con ITIL. Docente universitario con más de 22 años de experiencia en diferentes universidades nacionales y particulares a nivel de pregrado y postgrado. Docente en diferentes cursos de especialización en temas relacionados a: Auditoría Informática, Gestión de Riesgos de TI, Seguridad de la Información, Continuidad de negocio, Gobierno de TI y Gestión de servicios de TI. Auditor Informático, especializado en el sector financieras, con experiencia en más de 15 años. Proyectistas de proyectos informáticos a nivel de entidades públicas y privadas con experiencia en más de 20 años. Consultor externo en Gestión de servicios de TI. Cargos ocupados: Director de Escuela Profesional, Decano de Facultad, Presidente de Capítulo de CIP, Jefe de la Unidad de Riesgos de TI.

DATOS ACADÉMICOS

- **DOCTOR EN ADMINISTRACION**
  Universidad Nacional Pedro Ruiz Gallo

- **MAESTRO EN CIENCIAS INFORMÁTICA Y SISTEMAS**
  Universidad Nacional Pedro Ruiz Gallo

- **INGENIERO DE COMPUTACION Y SISTEMAS**
  Universidad Privada Antenor Orrego

EXPERIENCIA LABORAL

- **DIRECTOR DE ESCUELA**
  Universidad Nacional Pedro Ruiz Gallo
  ene. de 2016 – actualidad

- **DOCENTE UNIVERSITARIO**
  Universidad Nacional Pedro Ruiz Gallo

oct. de 1994 – actualidad

- **AUDITOR EXTERNO DE TI**
  Caja Rural De Ahorro Y Crédito Cruz De Chalpon (Hoy Caja Sipán)
  oct. de 2002 – dic. de 2015

- **PROYECTISTA PRINCIPAL**
  Consorcio ATA - KUKOVA
  nov. de 2009 – ago. de 2011

- **DECANO**
  Universidad Nacional Pedro Ruiz Gallo
  jul. de 2008 – jul. de 2011

- **LÍDER DE PROYECTO**
  Municipalidad Provincial Condorcanqui
  jun. de 2006 – nov. de 2006

- **DIRECTOR DE ESCUELA**
  Universidad Nacional Pedro Ruiz Gallo
  abr. de 2001 – set. de 2006

- **ANALISTA DE PROCESOS**
  Ministerio De La Producción
  jul. de 2004 – jul. de 2005

- **SUPERVISOR DE ELABORACIÓN DE EXPEDIENTE TÉCNICO**
  Proyecto Especial Olmos Tinajones
  abr. de 2002 – nov. de 2002

- **JEFE DE OFICINA CENTRAL**
  Universidad Nacional Pedro Ruiz Gallo
  may. de 2001 – dic. de 2001

JESSIE LEILA BRAVO JAICO

Docente en la UNPRG y en la USAT. Asesora y Consultora en TI. Especialista Redes, Seguridad y Auditoría Informática.

PERFIL

Ing. de Computación y Sistemas. Primera Promoción de la Universidad Privada Antenor Orrego de Trujillo. Doctora en Ciencias de Computación y Sistemas en la USS. Magister en Informática y Multimedia en la Universidad de Los Lagos - Chile. Magister en Administración de empresas con mención en Gerencia Empresarial de la Universidad Nacional Pedro Ruiz Gallo. Especialización en Redes Informáticas, Gestión de proyectos, Auditoría y consultoría de sistemas. Asesora y Consultora de TI en empresas de la región.

DATOS ACADÉMICOS

- **DOCTORA EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS**
  Universidad Señor De Sipán

- **MAESTRA EN ADMINISTRACIÓN CON MENCIÓN EN GERENCIA EMPRESARIAL**
  Universidad Nacional Pedro Ruiz Gallo

- **MAGÍSTER EN INFORMÁTICA Y MULTIMEDIA**
  Universidad San Pedro

- **INGENIERO DE COMPUTACIÓN Y SISTEMAS**
  Universidad Privada Antenor Orrego

- **CCNA - CISCO CERTIFIED NETWORK ASSOCIATE**

- **PMP – PROFESIONAL EN DIRECCIÓN DE PROYECTOS DEL PMI**

EXPERIENCIA LABORAL

- **CATEDRÁTICA**
  Universidad Nacional Pedro Ruiz Gallo
  oct. de 1994 – actualidad

- **CATEDRÁTICA**
  Universidad Católica Santo Toribio de Mogrovejo

ago. de 2000 – actualidad

- **CONSULTARA INFORMÁTICA**
  Clínica Servimédicos – AUNA
  jul. de 2006 – jul. de 2008

- **ASESORA Y CONSULTORA DE TI**
  Clínica MaxSalud
  ene. de 2004 – jul. de 2006

- **DIRECTORA DE ESCUELA**
  Universidad Nacional Pedro Ruiz Gallo
  set. de 1997 – dic. de 1999

GILBERTO CARRIÓN BARCO

Docente Posgrado en Universidad César Vallejo.

PERFIL

Doctor en Ciencias de la Computación y Sistemas. Maestro en Ingeniería de Sistemas, Magister en Docencia Universitaria. Ingeniero en Computación e Informática y Bachiller en Administración Pública, con Colegiatura N° 90931 por el Colegio de Ingenieros del Perú, habilitado. Consultor y Asesor en Soluciones de Networking y Servicios de Red para Gobiernos Locales y Regionales, con más de 13 años de experiencia en docencia universitaria en UNPRG, USS, UTP, USMP, USAT e Investigador en la línea Tecnologías de la Información, Gobierno Electrónico, Gestión por Procesos y Gestión por Resultados. Amplia experiencia como Jurado y Asesor de Investigaciones tanto en pregrado como en postgrado. Comprometido con el trabajo en equipo, proactivo y con vocación de servicio.

DATOS ACADÉMICOS

- **DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS**
  Universidad Señor De Sipán

- **MAESTRO EN INGENIERÍA DE SISTEMAS**

Universidad Nacional Pedro Ruiz Gallo

- **MAGISTER EN DOCENCIA UNIVERSITARIA**
  Universidad Privada César Vallejo

- **INGENIERO EN COMPUTACIÓN E INFORMÁTICA**
  Universidad Nacional Pedro Ruíz Gallo

- **CERTIFICACIÓN CISCO CCNA**
  Cisco

EXPERIENCIA LABORAL

- **DOCENTE POSGRADO**
  Universidad César Vallejo
  abr. de 2019 – actualidad

- **CATEDRÁTICO ASOCIADO**
  Universidad Tecnológica del Perú
  jun. de 2014 – actualidad

- **CATEDRÁTICO ASOCIADO**
  Universidad Nacional Pedro Ruiz Gallo
  ago. de 2006 – actualidad

- **CATEDRÁTICO ASOCIADO**
  Universidad Señor De Sipán
  abr. de 2006 – actualidad

- **DIRECTOR DE ESCUELA**
  Universidad Nacional Pedro Ruiz Gallo
  dic. de 2013 – ene. de 2016

- **GERENTE ADMINISTRATIVO**
  Centro de Entrenamiento en Tecnologías de la Información – CETI
  jul. de 2010 – dic. de 2015

- **CATEDRÁTICO ASOCIADO**
  Universidad de San Martin de Porres

ago. de 2010 – dic. de 2014

- **JEFE ÁREA ADMINISTRATIVA RED TELEMÁTICA**
  Universidad Nacional Pedro Ruiz Gallo
  jul. de 2010 – nov. de 2011

- **CATEDRÁTICO ASOCIADO**
  Universidad Católica Santo Toribio de Mogrovejo
  ago. de 2006 – dic. de 2009

HOBBER ARISTIDES SICCHA AYVAR

Gerente Corporativo de Tecnología de Información (CIO / CTO) en Grupo fe | Conductor de StarTICs | Leading Digital

PERFIL

Ejecutivo Senior con MBA - Administración Estratégica de Empresas por CENTRUM de la PUCP, Ingeniero de Computación y Sistemas, con más de 20 años de experiencia laboral en áreas de Innovación y Transformación Digital, Tecnología de la Información, Procesos, Proyectos, Talento Humano y Administración; en empresas transnacionales y nacionales del sector financiero, retail, educativo y de servicios. Líder en la formación de equipos eficaces e innovadores. También catedrático de posgrado, asesor y consultor.

Especialidades: Planeamiento estratégico de empresas, planeamiento estratégico de TIC, innovación y transformación digital, seguridad de la información, continuidad del negocio y metodologías de innovación y ágiles como: Design Thinking, XP, Kanban, así como experiencia de usuario: UX, UI.

DATOS ACADÉMICOS

- **MAGISTER EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS**
  Pontificia Universidad Católica Del Perú

- **INGENIERO DE COMPUTACIÓN Y SISTEMAS**
  Universidad Privada Antenor Orrego

- **ESPECIALIZACIÓN, MACHINE LEARNING**
  Massachusetts Institute of Technology

- **PROGRAMA EJECUTIVO DE TRANSFORMACIÓN DIGITAL**
  Universidad del Pacífico

- **ESPECIALIZACIÓN, GESTIÓN ESTRATÉGICA DE DATA**
  Escuela de Dirección de la Universidad de Piura

- **ESPECIALIZACIÓN, SEGURIDAD DE LA INFORMACIÓN**
  New Horizons Computer Learning Center of Raleigh-Durham-Chapel Hill

- **ESPECIALIZACIÓN, GERENCIA EN SEGURIDAD DE LA INFORMACIÓN**
  Universidad ESAN

- **ESPECIALIZACIÓN, BUSINESS INTELLIGENCE**
  Instituto Centroamericano de Administración de Empresas

- **MBA, MAGISTER EN ADMINISTRACIÓN ESTRATÉGICA DE EMPRESAS**
  CENTRUM Graduate Business School

- **DIPLOMA EN GESTIÓN EMPRESARIAL CON TI**
  Universidad ESAN

- **DIPLOMA EN ADMINISTRACIÓN DE TIC**
  Universidad ESAN

- **ESPECIALIZACIÓN, AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN**
  Contraloría General de la República del Perú

- **ISO 27001**
  PECB

EXPERIENCIA LABORAL

- **GERENTE CORPORATIVO DE TECNOLOGÍA DE LA INFORMACIÓN (CIO / CTO)**
  Campofe
  ene. de 2014 – actualidad

- **CATEDRÁTICO (PART TIME)**
  Universidad del Pacífico
  ago. de 2018 – actualidad

- **CATEDRÁTICO DE POSGRADO (PART TIME)**
  CENTRUM Graduate Business School
  ago. de 2016 – actualidad

- **CATEDRÁTICO DE POSGRADO (PART TIME)**
  Universidad Privada del Norte
  dic. de 2014 – actualidad

- **GERENTE DE PROCESOS Y PROYECTOS**
  Edpyme Marcimex
  abr. de 2011 – dic. de 2013

- **SUB GERENTE DE TECNOLOGÍA DE LA INFORMACIÓN**
  Inversiones La Cruz
  may. de 2010 – feb. de 2011

- **JEFE DE TECNOLOGÍA DE LA INFORMACIÓN Y ORGANIZACIÓN & MÉTODOS**
  Caja Rural de Ahorro y Crédito Sipán S.A.C
  mar. de 2007 – may. de 2010

- **CATEDRÁTICO**
  Universidad de San Martin de Porres
  mar. de 2008 – abr. de 2010

- **CATEDRÁTICO**
  Universidad Nacional Pedro Ruiz Gallo
  mar. de 2007 – dic. de 2007