

**Escuela Superior Politécnica del Litoral**

**Facultad de Ciencias Sociales y Humanísticas**

Diseño de un manual de procesos para gestión de contingencias en una empresa de comercialización de equipos industriales.

**Proyecto Integrador**

Previo la obtención del Título de:

**Licenciatura en Auditoría y Control de Gestión**

Presentado por:

Maitté Dayana Larcos Pizanán

Joseline Andrea Santillán Pincay

Guayaquil - Ecuador

Año: 2023

## Dedicatoria

---

Este proyecto está dedicado a mi familia en agradecimiento por el constante respaldo que me han dado en lo largo de mi vida, a mi mamá por ayudarme a salir adelante en mis estudios y a mi grupo favorito, Super Junior, porque gracias a su música encontraba la fuerza para sobrellevar los momentos duros de la carrera.

**Maitté Dayana Larcos Pizán.**

## Dedicatoria

---

Este trabajo es dedicado a mis padres quienes son un sostén indispensable en mi vida, su apoyo, amor y comprensión han sido mi mayor fortaleza e impulso para continuar ante los diversos obstáculos que se han presentado. A mi hermana quién a pesar de estar lejos ha sido mi mayor ejemplo y su enseñanza ha prevalecido en cada escalón de mi vida.

**Joseline Andrea Santillan Pincay.**

## Agradecimientos

---

Estoy agradecida con Dios, por alcanzar esta fase en mi vida.

A mis amigos quienes me alentaban a no rendirme y continuar adelante con la carrera.

A mis profesores por su enseñanza brindada a lo largo de mi vida académica.

Y a mi compañera Joseline Santillán por todo su esfuerzo y dedicación para lograr culminar este proyecto con éxito.

**Maitté Dayana Larcos Pizanán**

## Agradecimientos

---

Mi más sincero agradecimiento a Dios, mi guía constante en este arduo trabajo académico. Su guía, fortaleza y bendición han sido las bases sobre las cuales he culminado este proceso en mi vida.

Doy gracias a mis compañeros por sus constantes palabras de aliento y conocimientos compartidos en este proceso.

A mis profesores y tutores quienes han sido mi guía y han compartido conmigo su tiempo, dedicación y conocimientos.

Finalmente agradezco a mi compañera Maitté Larcos, por su dedicación, colaboración y paciencia a lo largo de este proyecto.

**Joseline Andrea Santillan Pincay.**

## **Declaración Expresa**

Nosotros Joseline Andrea Santillán Pincay y Maitté Dayana Larcos Pizanán acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores. La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

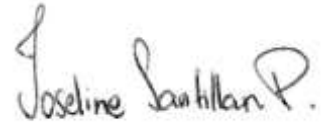
En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 31 de enero del 2024.

A handwritten signature in black ink on a light blue background. The signature reads "Maitte Arcos" in a cursive style.

---

**Maitté Dayana Arcos Pizán**

A handwritten signature in black ink on a white background. The signature reads "Joseline Santillán P." in a cursive style.

---

**Joseline Andrea Santillán Pincay**

## **Evaluadores**

---

**Benigno Alfredo Armijos De La Cruz**

**Profesor y Tutor de Materia  
Integradora**



## **Resumen**

En este proyecto actual se lleva a cabo la creación del diseño de un manual de procesos para gestión de contingencias que detalla los procedimientos a realizar durante la ocurrencia de una contingencia, así como el grupo responsable de cumplir con los lineamientos, canales de comunicación y los tiempos de inicio y fin que tomaría sobrellevar la contingencia presentada. El propósito del manual es ayudar al negocio con la continuidad de sus operaciones claves y a su vez proteger sus recursos humanos y materiales. La metodología empleada consiste en 8 fases: empezando por el levantamiento de información, entendimiento de los procesos, clasificación y consolidación de riesgos, evaluación de riesgo inherente, evaluación de controles, análisis del riesgo residual, estrategias y tratamiento y finalizando con el plan de acción. Los resultados obtenidos incluyeron los reconocimientos de riesgos críticos una vez aplicados los controles para posteriormente mitigarlos mediante la aplicación del manual. En conclusión, el uso del manual facilitará a la organización a responder de forma ágil y adecuada frente al impacto de una contingencia.

**Palabras Clave:** Contingencias, Gestión de Riesgos, Manual de procesos, Plan de Acción

## **Abstract**

This current project involves the creation of a contingency management process manual that details the procedures to be carried out during the occurrence of a contingency, and the group liable for complying with the guidelines, communication channels and the start and end times it would take to overcome the contingency presented. The purpose of the manual is to help the business with the continuity of its key operations simultaneously protect its human and material resources. The methodology employed consists of 8 phases: starting with information gathering, process understanding, risk classification and consolidation, inherent risk assessment, control assessment, residual risk analysis, strategies and treatment, and ending with the action plan. The results obtained included the recognition of critical risks once the controls had been applied and subsequently mitigated through the application of the manual. In conclusion, the use of the manual will help the organization to respond quickly and appropriately to the impact of a contingency.

**Keywords:** Contingency, Risk Management, Process Manual, Action Plan

## Índice General

Resumen.....	I
Abstract.....	II
Índice General.....	III
Índice de Tablas.....	V
Índice de ilustraciones.....	VI
Capítulo 1.....	I
1. Introducción.....	2
1.1 Descripción del problema.....	3
1.2 Justificación.....	3
1.3 Alcance.....	4
1.4 Objetivos.....	5
1.4.1 Objetivos generales.....	5
1.4.2 Objetivos Específicos.....	5
1.5 Marco Teórico.....	5
1.5.1 Marco Conceptual.....	5
Capítulo 2.....	13
2. Metodología.....	14
2.1 Levantamiento de Información.....	14
2.2 Entendimiento de los procesos.....	15
2.2.1 Diagrama Causa – Efecto.....	15
2.3 Clasificación y Consolidación de Riesgos.....	15
2.3.1 Riesgos Financieros.....	16
2.3.2 Riesgos Informáticos.....	16
2.3.3 Riesgos Operativos.....	16
2.3.4 Riesgos del Entorno.....	16
2.3.5 Riesgos Ocupacionales.....	16
2.4 Análisis del riesgo inherente.....	17
2.5 Evaluación de controles.....	19
2.6 Análisis del Riesgo Residual.....	20
2.7 Estrategias y tratamiento.....	22
2.8 Plan de Acción.....	23

Capítulo 3.....	24
3. Resultados y Análisis.....	25
3.1 Levantamiento de Información.....	25
3.1.1 Matriz de Riesgos: .....	25
3.2 Entendimiento de los procesos.....	27
3.3 Clasificación y Consolidación de Riesgos.....	27
3.3.1 Riesgos Financieros .....	28
3.3.2 Riesgos Informáticos .....	29
3.3.3 Riesgos Operativos .....	29
3.3.4 Riesgos del Entorno .....	30
3.3.5 Riesgos Ocupacionales .....	30
3.4 Análisis del riesgo inherente.....	31
3.5 Calificación de Controles.....	32
3.5.1 Propuesta de Controles, para riesgos con calificación 0.....	34
3.6 Riesgo Residual .....	35
3.7 Estrategias y tratamiento.....	37
3.8 Planes de Acción.....	38
3.8.1 Plan de acción 1: Caída de los sistemas informáticos.....	39
3.8.2 Plan de acción 2: Rotura de stock.....	39
3.8.3 Plan de Acción 3: Hurto, fraude, robo, asalto o ataques de extorsión .....	40
3.9 Análisis de Costos y Beneficios.....	41
3.9.1 Valoración de Costos .....	42
3.9.2 Valoración de Beneficios .....	43
Capítulo 4.....	45
4. Conclusiones y Recomendaciones.....	46
4.1 Conclusiones .....	46
4.2 Recomendaciones .....	47
5. Referencias .....	48

## Índice de Tablas

<b>Tabla 1</b>	Matriz de riesgo .....	17
<b>Tabla 2</b>	Niveles de riesgo.....	17
<b>Tabla 3</b>	Indicadores de probabilidad del riesgo .....	18
<b>Tabla 4</b>	Indicadores de impacto del riesgo.....	19
<b>Tabla 5</b>	Indicadores de evaluación de controles .....	19
<b>Tabla 6</b>	Indicadores para resultados de controles .....	20
<b>Tabla 7</b>	Descripción del tratamiento para los riesgos .....	22
<b>Tabla 8</b>	Valoración del riesgo inherente .....	31
<b>Tabla 9</b>	Valoración del control.....	33
<b>Tabla 10</b>	Propuesta de controles .....	35
<b>Tabla 11</b>	Valoración del Riesgo Residual .....	36
<b>Tabla 12</b>	Tratamiento por cada tipo de riesgo .....	37
<b>Tabla 13</b>	Plan de acción del riesgo 1 .....	39
<b>Tabla 14</b>	Plan de acción del riesgo 2 .....	39
<b>Tabla 15</b>	Plan de acción del riesgo 3 .....	41
<b>Tabla 16</b>	Costos .....	42
<b>Tabla 17</b>	Beneficios monetarios .....	43
<b>Tabla 18</b>	Otros beneficios .....	43

## Índice de ilustraciones

Ilustración 1	<i>Metodología aplicada</i> .....	14
Ilustración 2	<i>Nivel del Riesgo Residual</i> .....	21
Ilustración 3	<i>Mapa de Calor Riesgo Residual</i> .....	22
Ilustración 4	<i>Mapa de procesos</i> .....	26
Ilustración 5	<i>Diagrama de Ishikawa</i> .....	27
Ilustración 6	<i>Mapa de Calor Riesgo Inherente</i> .....	32
Ilustración 7	<i>Mapa de Calor Riesgo Residual</i> .....	37

## **Capítulo 1**

## **1. Introducción**

En 1957 la comercialización de hierro y sus derivados fue parte de las primeras actividades que desarrolló la empresa comercializadora de equipos industriales en el Centro Histórico de Quito, donde a raíz de diversas situaciones históricas la empresa experimentó cambios en su ubicación, personal y productos, que permitían reafirmar el compromiso que mantenían con sus clientes.

La empresa comercializadora de equipos industriales actualmente mantiene diversos servicios y productos que aportan soluciones constantes en los sectores productivos del país. Una de las principales actividades que permite que la empresa sea considerada por más de 66 años como una de las organizaciones más eficientes es la selección y montaje de bombas de agua en el Ecuador.

Dentro de la organización se encuentran departamentos claves y críticos que facilitan el progreso y la constancia de las actividades, las áreas de Crédito y Cobranzas, Logística y Comercial representan en la organización elementos fundamentales para el desarrollo de sus procesos, sin embargo, los mismo pueden enfrentar riesgos significativos durante situaciones inesperadas, de las cuales no se mantiene un registro o lineamientos a seguir para sobrellevar y garantizan el funcionamiento del negocio y la satisfacción de los consumidores.

El proyecto surge por la ausencia de una documentación que respalde y formalice los procesos ante eventos inesperados mediante directrices que determinen las actividades a realizar en estos casos. Por lo tanto, se plantea elaborar un manual de procesos para gestión de contingencias que contribuya a la continuidad de las actividades en las áreas consideradas críticas.



## **1.1 Descripción del problema**

Las empresas comerciales hoy en día se enfrentan a diversas amenazas que pueden derivarse de distintos factores y circunstancias específicas, tales como: problemas climáticos, crisis económicas, políticas, riesgos tecnológicos, salud pública, entre otros. En una situación crítica o contingencia, la empresa enfrenta el riesgo de que sus recursos operativos y comerciales puedan fallar, lo que podría tener un impacto negativo en sus actividades cotidianas y generar pérdidas a largo plazo. Esto incluiría la incapacidad para satisfacer la demanda de sus clientes, pérdidas de ingresos, daño o desprestigio para la marca y empresas relacionadas.

La pregunta central es: ¿Cómo se puede manejar y gestionar de forma efectiva los diversos riesgos que hoy en día afectan los procesos principales y críticos ante una situación emergente en la organización, de tal forma que se proporcionen procedimientos y protocolos claros que permitan a la empresa estar mejor preparada para enfrentar contingencias, minimizar impactos negativos y garantizar la continuidad de sus actividades?

Es importante mencionar que, por motivos de confidencialidad, no se revelará el nombre comercial del negocio donde se desarrollará el proyecto, sin embargo, para un mayor entendimiento denominaremos a la entidad como “Empresa comercializadora de equipos industriales”.

## **1.2 Justificación**

En el contexto actual donde las empresas enfrentan situaciones emergentes como contingencias durante un periodo de tiempo, reconocen estar en la necesidad de estar preparados para poder sobrellevar situaciones imprevistas y establecer de forma clara, precisa y coherente procedimientos que permitan a la empresa fortalecer su resiliencia empresarial y recuperarse de situaciones adversas. Es por esto que la herramienta que nos garantizará la continuidad de las

tareas en una compañía será la utilización del manual de procesos para contingencia, sin necesidad de pausar sus servicios y contacto con el cliente.

El manual de procesos constará de forma detallada con diversos lineamientos a seguir de acuerdo con el área o proceso crítico afectado, resaltando la contribución a la seguridad y bienestar de empleados de la empresa, así como los recursos que se emplean en ella. Además, se verificará el cumplimiento y disposición vigente que establecen las normas o políticas asociadas a la gestión de riesgos en la compañía, ya sean internas o externas y se espera que la implementación de este manual en la empresa refleje de forma efectiva la asignación de roles, responsabilidades, recursos y estrategias emergentes que permitan la continuidad de las actividades afectadas y restauración de insumos y maquinarias en riesgo.

### **1.3 Alcance**

Esta iniciativa se llevará a cabo en los departamentos de Crédito y Cobranzas, Logística y Abastecimiento y Comercial de la empresa. El estudio se enfocará en los procesos críticos determinados en la matriz de riesgo en el que se analizarán las etapas y el personal involucrado en cada una de las actividades. Los recursos a utilizar comprenden información proporcionada por los responsables de cada área como fuente primaria, quienes proveerán la información y retroalimentación respectiva. Asimismo, se tendrán en cuenta la revisión de normativas legales vigentes relacionadas con la gestión y evaluación de riesgos. Finalmente, para la culminación del proyecto habrá un periodo de tiempo comprendido entre el 16/10/2023 hasta el 16/01/2024

## 1.4 Objetivos

### 1.4.1 *Objetivos generales*

Elaborar un manual de procesos de contingencias en una empresa comercial, a través de la recolección de información y el análisis de riesgos, con el propósito de garantizar la continuidad de sus operaciones comerciales, técnicas, logísticas y salvaguardar los recursos organizativos

### 1.4.2 *Objetivos Específicos*

- i. Efectuar una recopilación de datos y documentos asociados con la matriz de riesgos de la empresa para identificar los procesos críticos y oportunidades de mejora en las áreas correspondientes.
- ii. Analizar los riesgos críticos relacionados con los procesos claves de la organización para definir su tratamiento y planes de acción oportunos.
- iii. Desarrollar un manual de procesos de contingencia para una organización de comercialización de equipos industriales, donde se detallan las funciones y deberes del equipo de gestión y de los empleados durante situaciones de contingencia.

## 1.5 Marco Teórico

### 1.5.1 *Marco Conceptual*

#### **i. Contingencia**

Contingencia se puede definir como una condición que ocurre de forma imprevista en el futuro con capacidad de ocasionar problemas dentro de las organizaciones (Westreicher, 2020).

En la teoría de contingencia se examina cómo las organizaciones responden a distintas condiciones ambientales que son influenciadas por factores externos, los cuales afectan la gestión de sus operaciones internas (Bueren & Fiorentin, 2014).

Esta teoría expone que, dentro de una organización, es necesario afrontar los desafíos y tener en cuenta dos categorías de variables: aquellas relacionadas con factores internos y externos del entorno. Es crucial establecer cómo estas variables se vinculan con los procesos administrativos u operativos (Mora Lema, 2011).

## **ii. Mitigación**

Planificación y aplicación de medidas dirigidas a reducir riesgos, dado que, en muchos casos no se puede prevenir riesgos o contingencias para evitar pérdidas y efectos adversos, sino solo es posible suavizar su impacto (Lavell, 2001).

Establecer políticas para la reducción de riesgos ayuda a optimizar la calidad de los procesos internos, además de contribuir a la continuidad de las organizaciones (Rodríguez López, Piñeiro Sánchez, & de Llano Monelos, 2013).

## **iii. Mapa de procesos**

Herramienta visual donde se presentan actividades relacionadas con procesos de toda la empresa, los cuales están clasificados en estratégicos, operacionales y de soporte para entregar el producto o servicio ofertado al usuario final (Alonso , 2023).

Los procesos estratégicos están vinculados a las políticas, reglas y estrategias definidas por la entidad. Por otro lado, los procesos operativos abarcan las actividades indispensables para proporcionar un bien o servicio valioso, mientras que los procesos de soporte ofrecen el respaldo necesario para llevar a cabo estas actividades productivas (Pico, 2006).

Es relevante señalar que un mapa de procesos también se puede entender como un esquema de macroprocesos, ya que en él se presenta información generalizada con procesos extensos pero definidos de manera concisa. Además, cada mapa de procesos es único, ya que la

información que contiene sobre cada empresa varía en función de sus objetivos y actividades particulares (Alarcón et al., 2019).

#### **iv. Manual**

Miguel A. Duhalt Kraus conceptualiza el manual como un registro que presenta de manera estructurada y sistemática información e instrucciones relacionados a los procesos, normas e historia de una empresa. Estos elementos se consideran esenciales para mejorar el desarrollo efectivo del trabajo, según Fustillos Parra (2010) citando a Duhalt (1977).

Se define un manual como la presentación formal de todas las indicaciones e información esencial para llevar a cabo operaciones en un sector específico. Funciona como una guía que orienta correctamente las acciones del personal operativo hacia la dirección apropiada Zetina-Bautista, Huicab-García, & Coop-Abreu, (2021) citando a Continolo (1984),

#### **v. Manual de procesos de contingencias**

Un manual de procesos para contingencias es una guía de instrucciones que abarcan todos los procesos realizados en las áreas críticas de una empresa, que están susceptibles a diversos tipos de riesgos. Su objetivo es establecer políticas, funciones y responsabilidades específicas, para agilizar las operaciones y prevenir pérdidas en la empresa por diversos riesgos (Asanza Molina, Miranda Torres, Ortiz Zambrano, & Espín Martínez, 2016).

#### **vi. Metodología del riesgo**

Secuencia y estudio de procedimientos que se utilizan para evaluar e identificar riesgos, su estudio, control y tratamiento (Pardinas, 1989).

La metodología es un grupo de indicaciones o métodos operativos que se desarrollan a partir de la indagación para alcanzar un objetivo, mediante el cual se aplican distintos métodos y fases de indagación. (Gómez Vargas, Galeano Higueta, & Jaramillo Muñoz, 2015)

Además, es importante utilizar una metodología del riesgo para transformar la información inicial de una forma más estructurada y concreta (Mora Lema, 2011).

#### **vii. Matriz de riesgo**

Es un instrumento empleado para reconocer y gestionar los riesgos netos a las operaciones de una empresa. Su utilidad se extiende a diversas situaciones y procesos, lo que la convierte en un instrumento efectivo para reforzar la seguridad empresarial (Mora Horta , 2016).

La matriz de riesgos no solo se ocupa de reducir los riesgos en la empresa, sino también de asignar y reconocer los recursos necesarios para las áreas con mayores riesgos o procesos críticos, con el fin de lograr una gestión y medición efectivas. (Madrid Nicolás & Serrano Madrid, 2019)

Esta herramienta es actualizada por la empresa comercializadora de equipos industriales cada 3 meses, su propósito es detectar posibles riesgos en las operaciones desarrolladas en cada área significativa.

#### **viii. Impacto**

Es la magnitud con la que un riesgo impacta de forma negativa al negocio y las consecuencias que ocasiona (López Serrazina, Jiménez Ayala, & Catató Alis, 2023).

#### **ix. Probabilidad**

Se entiende como una eventualidad o potencialidad, susceptible de especificarse, evaluarse o establecerse de manera objetiva y subjetiva. Esta evaluación puede realizarse de forma cualitativa o cuantitativa, utilizando descripciones que abarquen desde términos generales hasta enfoques matemáticos rigurosos (International Organization for Standardization, 2018).

#### **x. Continuidad del negocio**

Una compañía que posee una estructura de gestión de continuidad eficiente está preparada para hacer frente a interrupciones. Esto resulta ventajoso en sectores donde cualquier interrupción en un proceso crucial podría tener repercusiones significativas en el personal o en el ámbito financiero, incluyendo áreas como servicios gubernamentales, de salud, financieros, defensa y sociales ( International Organization for Standardization, 2019).

De igual manera la norma establece los principios esenciales a considerarse para la continuidad del negocio, que consta en 5 partes empezando por las obligaciones y deberes de parte de la dirección de la entidad, determinar objetivos claros que respalde la gestión para la continuidad, conocer el impacto y evaluar los riesgos, comunicación con los usuarios interesados tanto como internos y externos y pruebas periódicas para conocer la efectividad del plan de continuidad.

#### **xi. Control interno**

El Control Interno engloba el procedimiento establecido por la administración y los empleados de una entidad con el fin de garantizar un nivel apropiado de protección para lograr metas vinculadas con: la precisión de los datos económicos de la entidad, el acatamiento de las normas vigentes y el desarrollo eficaz de las tareas (COSO, 2019).

El control interno es una gestión integral establecido por el líder máximo, la administración y los empleados de cualquier organización, a fin de verificar el alcance de las metas corporativas y la preservación del financiamiento estatal. Los elementos esenciales del control interno abarcan la supervisión del entorno, los mecanismos de información y comunicación, así como los procedimientos de seguimiento. (Contraloría General del Estado, 2023).

Ambas referencias coinciden en la idea central del control interno como un proceso sistemático liderado por la gerencia y los empleados de una organización. Además, destacan la importancia de este proceso para asegurar un nivel apropiado de seguridad en el alcance de los objetivos institucionales. Estas expresiones comparten la preocupación por aspectos fundamentales del control interno, como la veracidad de la información económica, acatamiento de las normativas correspondientes y la eficacia y eficiencia en las operaciones.

#### **xii. Sistema de planificación de recursos empresariales (ERP)**

El ERP, es una plataforma de gestión integrada que posibilita a una entidad optimizar y estandarizar sus procesos. Es un software importante debido a la facilidad en la que proporciona a los usuarios información transparente, confiable e integrada (Abdullah, 2017 ).

Además, este sistema se considera de forma práctico y viable, dado que permite intercambiar y difundir información privada entre los colaboradores de la organización. La implementación de este sistema se establece en 6 fases progresivas: análisis de viabilidad, planificación, modelado, ajuste de parámetros, ejecución y activación del sistema informático (Acosta Vega, Ospino Ayala, & Valencia Espejo , 2017).

La no aplicación del sistema y la falta de aprovechamiento del mismo minimiza y dificultaría el cumplimiento de fines y objetivos planificados en la compañía (Iacub, 2015).

#### **xiii. ISO 31000:2018**

Norma Internacional cuyo propósito es la Gestión de Riesgo, que ofrece instrucciones o un procedimiento a seguir para administrar los riesgos que pueden presentarse en la organización, estas directrices se caracterizan por ser flexibles y adaptables a cualquier entorno para mejorar el desempeño y alcanzar metas de una manera eficaz, a través de sus cláusulas, debido a que, las empresas sin importar su naturaleza o dimensión se ven confrontadas por influencias iterativas



que generan incertidumbre en la funcionalidad de procesos, capacidad para lograr objetivos y satisfacción al cliente. Fue creada en 2009 y su relevancia trasciende las fronteras de la industria, ya que todas las organizaciones pueden enfrentar desafíos relacionados con el bienestar, resguardo y medio ambiente. El propósito primordial del manejo de riesgos se centra en el reconocimiento y reducción de amenazas en todas las áreas operativas, contribuyendo así a la protección de los colaboradores. Algunos factores fundamentales de la norma ISO 31000 son:

1. Marco de referencia: Proporciona directrices generales para la gestión del riesgo, considerando aspectos como el liderazgo, la integración, el diseño, la implementación, la valoración y la mejora.
2. Proceso: Describe cómo llevar a cabo el manejo del riesgo, incluyendo la comunicación.
3. Cambios en la revisión de 2018:
  - Mayor atención al liderazgo.
  - Consideración de riesgos en la toma de decisiones.
  - Énfasis en una aplicación efectiva.
  - Estandarización del lenguaje.
  - Uso de información precisa y actualizada.

Además, previene posibles sanciones y multas derivadas de estas situaciones (International Organization for Standardization, 2018).

#### **xiv. ISO 22301**

Esta norma, publicada en 2019 por la Organización Internacional de Estandarización (ISO), describe las directrices para los sistemas de gestión de la continuidad del negocio. Su intención es garantizar que las organizaciones puedan mantener sus operaciones ante crisis como desastres naturales, ciberataques o pandemias. Aplicable a organizaciones de cualquier tamaño o

sector, la norma consta de 10 secciones que especifican requisitos como el alcance del sistema, responsabilidades de la alta dirección, planificación, soporte, implementación y operación del sistema, evaluación del desempeño y mejora continua ( International Organization for Standardization, 2019).

#### **xv. Políticas internas de la Empresa Comercializadora de Equipos Industriales**

Son directrices que mantiene la Empresa Comercializadora de Equipos Industriales para regular las normas de conducta para los miembros de la entidad, las políticas internas van alineadas con: Recursos Humanos, Ética y conducta empresarial, Seguridad y Salud ocupacional, Tecnología, Medio ambiente, Servicio al cliente, Cumplimiento legal y Gestión de riesgos. Además, contribuye a asegurar el cumplimiento de todas las operaciones de la compañía.

#### **xvi. COSO Marco de Gestión de Riesgo**

Es una organización privada e independiente que desarrolló e implementó un marco COSO cuyo propósito es ayudar a la organización a establecer y evaluar el monitoreo interno. Este sistema garantiza el alcance de resultados de la organización, ayuda a identificar, evaluar y gestionar riesgos, mejora la productividad y protege los bienes y patrimonios de la organización a largo plazo de una manera sostenible. Además, se encuentra estrechamente relacionado al sistema de gestión de riesgo, debido a que el marco COSO ERM establece lineamientos para administrar y mitigar de forma efectiva el riesgo presentado, promoviendo de esta manera una cultura de riesgo a los colaboradores de la empresa, para que se comprenda la relevancia de la estructura del riesgo (Ambrosone, 2007).

## Capítulo 2

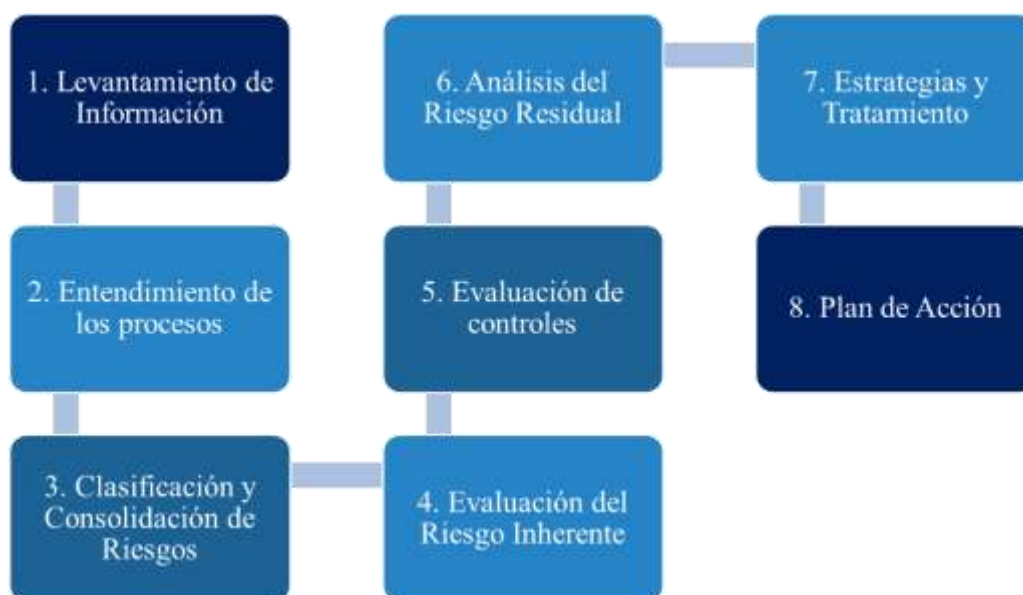
## 2. Metodología.

Como metodología se describe minuciosamente un enfoque sistemático, ofreciendo un enfoque sistemático para abordar los objetivos propuestos. La siguiente metodología aborda las técnicas de investigación, la recopilación y análisis de datos, junto a otros procedimientos que permitirá asegurar la integridad y confiabilidad de los resultados.

La metodología del presente proyecto se encuentra estructurado en 8 fases, que se describen en la ilustración 1:

### Ilustración 1

*Metodología aplicada*



*Fuente:* Elaboración propia

### 2.1 Levantamiento de Información

Este apartado se ejecutó a través de reunir información relevante que mantiene la empresa, con el propósito de establecer un entendimiento global de los procesos desarrollados en cada área. Esta etapa fue fundamental para el análisis del negocio, y la herramienta que se utilizó fue investigación exploratoria, observación y reunión con la coordinadora de aseguramiento de la

calidad, mediante la primera reunión en las instalaciones de la organización el 26 de octubre del 2023, donde se obtuvo información detallada sobre el manejo y logro de los objetivos planteados para cada área crítica, a través del análisis de herramientas visuales como:

- Matriz de riesgos
- Organigrama
- Mapa de procesos

## **2.2 Entendimiento de los procesos**

### **2.2.1 Diagrama Causa – Efecto**

La herramienta del gráfico de Ishikawa, también reconocida como espina de pescado, posibilita la identificación del punto de origen de un conflicto (Bravo Arias, 2022).

Esto tiene como propósito optimizar los procedimientos y recursos dentro de una compañía, abarcando aspectos como los recursos humanos, materiales, financieros e intangibles, al igual que Rodríguez Gallego & Ordóñez Sierra (2012) citando a Amsden y Robson (2004).

El análisis de Relación de Causa-Efecto se lleva a cabo a través del esquema de Ishikawa donde se busca visualizar un resultado poco satisfactorio (Efecto) y descubrir los elementos (Causas) responsables de su origen.

Luego de analizar la matriz de riesgo, se realizó una lluvia de ideas para construir el diagrama de causas, donde se consideró cinco aspectos los cuales se dividen en: personas, medición, método, medio ambiente y materiales

## **2.3 Clasificación y Consolidación de Riesgos**

Después de analizar la matriz de evaluación de riesgos proporcionada y elaborada por la organización comercial, se identificó aquellos riesgos con un nivel de impacto significativo y que conllevarían mayores pérdidas para la empresa. Por lo tanto, estos riesgos fueron clasificados

según su tipo en relación al área para gestionarlos de manera efectiva y obtener una visión integral de la exposición que mantiene la organización:

### **2.3.1 Riesgos Financieros**

Los riesgos financieros afectan al alcance económico establecido por la organización, teniendo un impacto negativo en los ingresos y flujo del efectivo, relacionado con la variabilidad de los mercados y obligaciones financieras, tasas de interés, entre otros.

### **2.3.2 Riesgos Informáticos**

Este tipo de riesgo involucra la amenaza a los recursos informáticos de la organización, estos riesgos pueden tener un impacto significativo en la reserva, coherencia y accesibilidad de los datos demandan su análisis y administración con el propósito de preservar los datos y el intercambio en tecnologías digitales.

### **2.3.3 Riesgos Operativos**

Son aquellos riesgos que afectan al rendimiento operativo en las áreas de la empresa, los cuales permiten analizar la posibilidad de pérdidas resultantes de deficiencias en los procesos internos.

### **2.3.4 Riesgos del Entorno**

En esta categoría se encuentran aquellos riesgos que no pueden ser controlados por la empresa, que provienen de factores externos e impactan significativamente en las operaciones y el rendimiento de la entidad, por lo que es necesario anticipar sus posibles impactos y desarrollar estrategias o planes para mitigar los riesgos.

### **2.3.5 Riesgos Ocupacionales**

Son aquellos riesgos que afectan el bienestar del colaborador por incumplimiento de normas o políticas internas, causados por condiciones inadecuadas del colaborador o factores

psicosociales como el estrés laboral, entre otros. La administración de contratiempos ocupacionales permite supervisar los riesgos existentes con la finalidad de brindar un espacio laboral donde se vela por la seguridad de los colaboradores.

## 2.4 Análisis del riesgo inherente

En esta fase de la gestión de riesgos se evaluó el riesgo intrínseco de cada actividad, prescindiendo de los mecanismos de control. El propósito fundamental del análisis del riesgo inherente es entender la naturaleza del riesgo, su impacto y la probabilidad de su ocurrencia. Este procedimiento se implementó mediante el estudio de la matriz de riesgo de la entidad mercantil enfocada en la venta de productos industriales, que asigna una puntuación cuantitativa de 1 a 5 y establece un nivel cualitativo de riesgo categorizado como crítico, alto, medio y bajo. La meta es establecer la relevancia relativa de los riesgos y dar prioridad a las medidas de manejo de riesgos.

**Tabla 1**

*Matriz de riesgo*

	IMPACTO				
PROBABILIDAD	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

*Fuente:* Empresa Comercial de equipos industriales

**Tabla 2**

*Niveles de riesgo*

DESCRIPCIÓN
1 – 3      Bajo

4 – 10	Medio
11- 16	Alto
17-22	Crítico
23-25	Catastrófico

*Fuente:* Empresa Comercial de equipos industriales

Conforme a la tabla, se evaluó el efecto global de los riesgos en la empresa utilizando una escala numérica del 1 al 5, donde 1 indica el impacto mínimo y 5 el máximo. El número seleccionado se multiplicó por la oportunidad de ocurrencia, también evaluada en un rango del 1 al 5, donde 1 indica la probabilidad mínima y 5 la más elevada. El resultado de multiplicar estas dos variables se empleó para calcular el nivel de gravedad del riesgo.

Para dar una valoración al efecto y la posibilidad de los riesgos, la empresa determinó los siguientes indicadores:

**Tabla 3**

*Indicadores de probabilidad del riesgo*

<b>Probabilidad</b>	<b>Tipo de posibilidad</b>	<b>Frecuencia (cada n° días)</b>
1	Extremadamente rara	Nunca ha sucedido
2	Rara	Se puede presentar una vez cada tres años o menos de una vez al año
3	Probable	Se puede presentar una o dos veces al año
4	Altamente probable	Se puede presentar de tres a doce veces al año (una por mes)
5	Casi seguro	Se puede presentar más de una vez al mes

*Fuente:* Empresa Comercial de equipos industriales



**Tabla 4***Indicadores de impacto del riesgo*

<b>Impacto</b>	<b>Tipo de impacto</b>	<b>Costo</b>
1	Insignificante	Menos de \$500
2	Menor	Entre \$500 y \$ 2.500
3	Moderado	Entre \$ 2.500 y \$ 12.500
4	Importante	Entre \$ 12.500 y \$ 62.500
5	Catastrófico	Más de \$62.500

*Fuente:* Empresa Comercial de equipos industriales**2.5 Evaluación de controles**

La evaluación de controles son procesos internos que permiten a la empresa comercializadora prevenir desviaciones a fin de lograr sus objetivos, para el establecimiento de los controles se determinó el criterio del control de acuerdo con el tipo, implementación, evidencia y cumplimiento, para este estudio se utilizó una matriz de criterio de evaluación de controles con una calificación de acuerdo con sus pesos y porcentajes, a fin de establecer un resultado cuantitativo mínimo 0 y máximo 100, el cual será utilizado para determinar el valor del riesgo residual.

**Tabla 5***Indicadores de evaluación de controles*

<b>Criterio del Control</b>	<b>%</b>	<b>Categoría</b>	<b>Peso</b>
Implementación	10 %	Automático	70
		Manual	30
Tipo	20 %	Preventivo	40
		Detectivo	30
		Correctivo	30
Evidencia		Evidencia del control-Documentado	80

	20 %	Sin evidencia del control- no documentado	20
Cumplimiento	50 %	Control no revisado	5
		Control no implementado o no se aplica	20
		Control funciona de manera efectiva	75

*Fuente:* Dirección de Gestión y Desempeño Institucional, 2022, págs. 47 - 48

De acuerdo con la tabla, primero se evaluó el control en relación a su criterio, luego se seleccionó la categoría que describe el control con su peso para multiplicar dicho valor con el porcentaje del criterio, obteniendo como resultado una calificación ponderada al 100%.

Calificación que fue categorizada de acuerdo al rango establecido a continuación:

### Tabla 6

*Indicadores para resultados de controles*

Mínimo	Máximo	Calificación	Resultado Control
0	20	1	Muy Bajo
21	40	2	Bajo
41	60	3	Moderado
61	80	4	Fuerte
81	100	5	Robusto

*Fuente:* Elaboración propia

## 2.6 Análisis del Riesgo Residual

El riesgo residual es considerado a aquellos riesgos que permanecen aún después de haber implementado los controles respectivos de acuerdo con el nivel de criticidad del riesgo inherente. Una vez identificada la calificación cualitativa de los controles se procedió a relacionar dicha calificación con el valor cualitativo de los riesgos inherentes, obteniendo de esta forma la valoración del riesgo residual explicada en la ilustración:

## Ilustración 2

### *Nivel del Riesgo Residual*

Nivel de Riesgo Inherente	Resultado de control de Riesgo	Nivel de Riesgo Residual
Bajo	Muy bajo	Bajo
Bajo	Bajo	Bajo
Bajo	Moderado	Bajo
Bajo	Fuerte	Bajo
Bajo	Robusto	Bajo
Medio	Muy bajo	Medio
Medio	Bajo	Medio
Medio	Moderado	Bajo
Medio	Fuerte	Bajo
Medio	Robusto	Bajo
Alto	Muy bajo	Alto
Alto	Bajo	Alto
Alto	Moderado	Medio
Alto	Fuerte	Medio
Alto	Robusto	Medio
Crítico	Muy bajo	Extremo
Crítico	Bajo	Extremo
Crítico	Moderado	Alto
Crítico	Fuerte	Alto
Crítico	Robusto	Alto
Catastrófico	Muy bajo	Extremo
Catastrófico	Bajo	Extremo
Catastrófico	Moderado	Extremo
Catastrófico	Fuerte	Extremo
Catastrófico	Robusto	Extremo

*Fuente:* Elaboración propia

Una vez que se determinó la calificación del riesgo residual, se procedió a evaluar el riesgo operativo a través de un mapa de calor, el cual nos permitió visualizar con mayor precisión la criticidad del riesgo y su posterior tratamiento.

### Ilustración 3

*Mapa de Calor Riesgo Residual*

	RIESGO INHERENTE				
CONTROL	Bajo	Medio	Alto	Crítico	Catastrófico
Muy bajo					
Bajo					
Moderado					
Fuerte					
Robusto					

*Fuente:* Elaboración propia

## 2.7 Estrategias y tratamiento

En esta sección, se evaluaron las estrategias de respuesta correspondientes a cada riesgo operacional identificado, considerando el grado de exposición de cada riesgo, para determinar la acción o tratamiento más apropiado según la caracterización del riesgo de la organización.

El tratamiento de las vulnerabilidades se estableció en relación a los siguientes factores:

**Tabla 7**

*Descripción del tratamiento para los riesgos*

Tipo	Perfil del Riesgo	Descripción
Aceptar	Aceptación	Cuando la organización puede tolerar el riesgo, debido a pérdidas mínimas.
Reducir/ Mitigar	Límite de Riesgo	Cuando la acción permite reducir el impacto a la frecuencia del riesgo
Evitar el riesgo	No aceptable	Cuando el proceso o producto evaluado no se

---

elige para su producción o implementación debido a tener un nivel de riesgo elevado

---

*Fuente:* Matriz de Riesgo de la empresa comercializadora

La tabla 7 muestra el grado de aceptación del riesgo residual, considerando el tratamiento adecuado y la perspectiva completa de la compañía, esta herramienta permite decidir en cuanto a la aceptación y tolerancia del riesgo, con el propósito de poner en marcha un plan de acción enfocado a los riesgos más significativos de la empresa.

## **2.8 Plan de Acción**

Se describió que acciones se seguirán ante los riesgos de la empresa, el período estimado en que deberían ejecutarse cada acción, los tiempos de recuperación, los recursos a utilizar, indicadores y los responsables de rastrear y controlarlas, considerando los riesgos que pueden ocasionar interrupciones en las actividades de la empresa.

- **Acciones:** Detalle de las medidas a realizar de forma preventiva de los riesgos seleccionados.
- **Fecha límite de implementación:** Detalle de fecha donde debería ya haberse ejecutado el plan de acción.
- **Recursos:** Elementos o recursos requeridos para ejecutar las funciones programadas en el plan de acción y lograr los objetivos definidos.
- **Responsables:** Encargados de que las acciones propuestas sean cumplidas en el periodo establecido.

### **Capítulo 3**

### **3. Resultados y Análisis**

#### **3.1 Levantamiento de Información**

Como primera reunión con la coordinadora de aseguramiento de la calidad de la entidad comercializadora de equipos industriales se estableció de forma clara y sencilla los procedimientos e historia de la organización, explicando la metodología, normativa, relación con las áreas, clientes, proveedores, infraestructura y riesgos a los que están expuestos sus colaboradores.

Para un mayor entendimiento se recopiló información a través de preguntas y análisis de herramientas que definen la gestión con la que se maneja la empresa, y se obtuvo como resultado de sus herramientas lo siguiente:

##### **3.1.1 Matriz de Riesgos:**

La empresa en mención se mantenía expuesta a una serie de riesgos, entre los que se encontraban:

- i.** Riesgos financieros: Relacionados a créditos a clientes y cuentas incobrables.
- ii.** Riesgos informáticos: Problemas que afectaban el sistema de la empresa.
- iii.** Riesgos operativos: Problemas con la logística y almacenamiento de productos.
- iv.** Riesgos ambientales: cambios climáticos que dañan la infraestructura y su entorno.
- v.** Riesgos ocupacionales: Riesgos relacionados al incumplimiento normativo que atenta a la cultura y genera peligro para los colaboradores.

Estos imprevistos ocasionaban con frecuencia que las actividades de la organización fueran interrumpidas, afectando su productividad y rentabilidad.

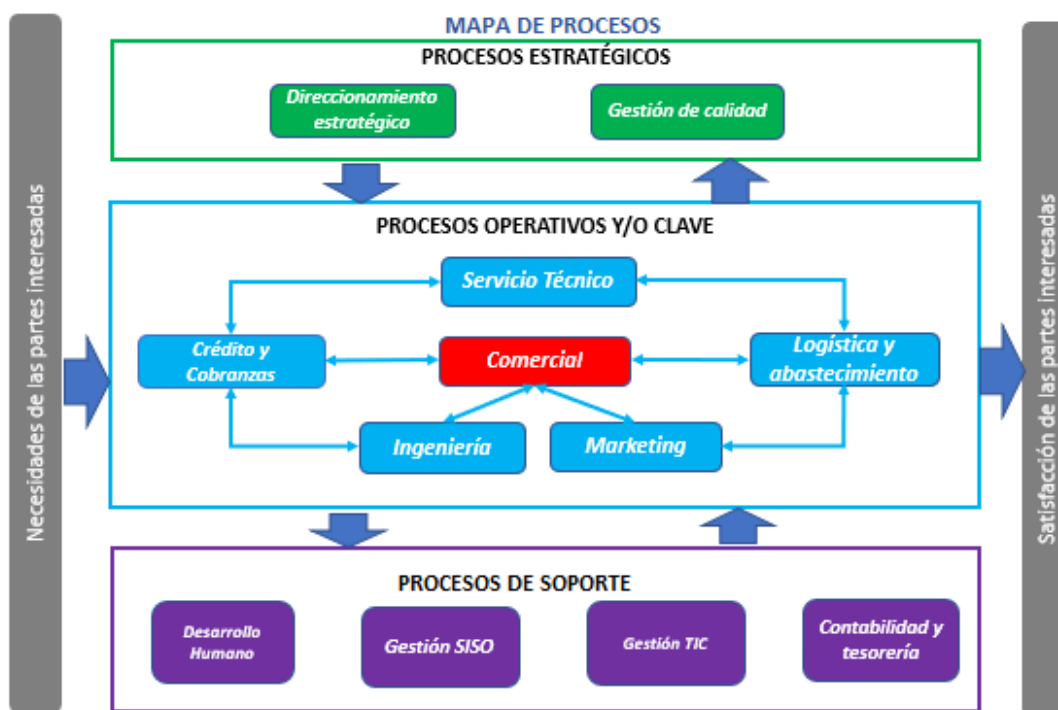
### 3.1.1 Mapa de Procesos:

La organización de productos industriales mantiene procesos estratégicos que otorgan direccionamiento y gestión de la calidad. Estos procesos contienen procedimientos claves que satisfacen las necesidades de las partes interesadas, como servicio técnico, crédito y cobranzas, logística y almacenamiento, ingeniería y marketing.

Los procesos claves, a su vez, se apoyan en el soporte de área de desarrollo humano, gestión SISO, gestión TIC y contabilidad y tesorería.

#### Ilustración 4

*Mapa de procesos*



*Fuente:* Empresa de comercialización de equipos industriales

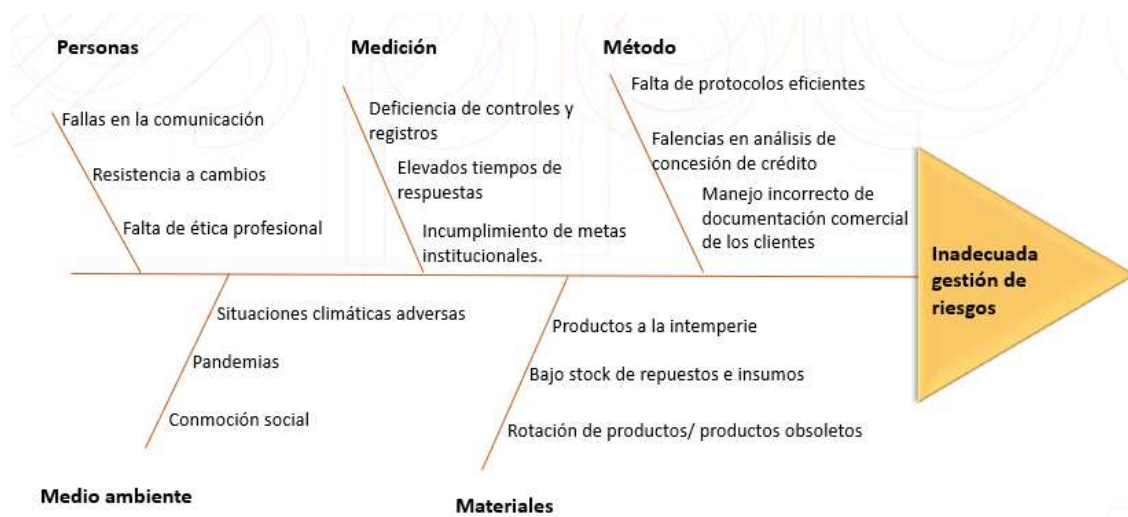


### 3.2 Entendimiento de los procesos

Con el propósito de comprender los procesos, se evaluó la información recopilada, identificando las actividades fundamentales que contribuyen a la entrega del producto final. Como resultado, se pudo constatar que en la empresa comercial de equipos industriales existe una gestión de riesgos deficiente. De esta manera, se decidió crear un gráfico con el fin de identificar las potenciales razones y consecuencias de esta situación específica, simplificando de esta manera el proceso de elección para enfrentar la circunstancia de manera eficiente.

#### Ilustración 5

Diagrama de Ishikawa



Fuente: Elaboración propia

Como principal causa identificada se determinó es la falta de protocolos eficientes en la organización que permita detallar, respaldar y formalizar procedimientos claros durante una contingencia.

### 3.3 Clasificación y Consolidación de Riesgos

Una vez que se determinaron los tipos de riesgos que serían considerados para el análisis de este trabajo, se identificó los riesgos con mayor criticidad, de acuerdo con la matriz

proporcionada por la empresa. Para ello, se categorizaron los riesgos según su relación con los tipos establecidos, tales como se muestran a continuación:

### 3.3.1 *Riesgos Financieros*

#### *Proceso: Comercial*

- **Imposibilidad de vender a entidades públicas por incumplimiento de contratos:** La empresa en mención está sujeta a ciertas obligaciones y requisitos, entre ellas celebrar contratos con entidades públicas, si la empresa comercializadora de equipos industriales no cumple con dicho requisito se enfrentará a sanciones de entes gubernamentales e interrupción de sus operaciones con el sector público durante cinco años, esta consecuencia se da origen por la ausencia de suministros claves y errores en el manejo de la documentación.

- **Pérdida financiera por fuga de clientes:** Los clientes existentes de la empresa dejarán de realizar negocios con la empresa comercializadora de equipos industriales y en su lugar erigirán productos o servicios de un competidor, debido a la aparición de competencia “low cost”, es decir empresas que ofrecen servicios o productos similares con un precio menor. Además, la fuga de clientes se puede originar por la baja rotación de stock, malos tratos hacia el cliente, elevados tiempos de respuestas y disminución del poder adquisitivo de los clientes, desarrollando de esta forma pérdidas económicas y oportunidades comerciales.

#### *Proceso: Crédito y Cobranzas*

- **Incobrabilidad de cuentas:** La empresa comercializadora de equipos industriales puede enfrentarse en la situación en la que no podrá recuperar los pagos pendientes de sus clientes, debido a la presión que existe de comercial para que se venda mercadería a clientes morosos y por la falencia en el análisis para concesión del crédito, esto puede traer como consecuencia pérdidas económicas para la empresa.

- **Concesión de créditos a clientes con baja capacidad de pago:** La empresa al otorgar créditos a clientes cuya capacidad financiera para cumplir con los términos de pago es limitada durante los plazos acordados puede traer como consecuencia pérdidas económicas e incomodidad del cliente dado a que no se está cumpliendo con el proceso de venta establecido por la deficiencia en la recolección de soportes para la validación crediticia que existe en la empresa.

### 3.3.2 *Riesgos Informáticos*

*Proceso: TICS*

- **Caída de los sistemas informáticos:** La empresa comercial ha sufrido en dos ocasiones la caída de sus sistemas informáticos debido a la generación de códigos maliciosos, hackeos y delitos cibernéticos, que pueden ocasionar demoras en el servicio, interrupciones en las operaciones y a su vez pérdidas económicas a corto plazo, generando de esta forma molestia en sus clientes frecuentes.

### 3.3.3 *Riesgos Operativos*

*Proceso: Logística y Abastecimiento*

- **Rotura de stock:** La empresa en mención en ocasiones puede verse en la situación de no contar con el nivel de inventario suficiente para atender las necesidades de los clientes, esto se debe a la interrupción en el suministro de materia prima y que en ocasiones el proveedor no dispone de stock del producto en el momento requerido.
- **Retraso en la importación de la mercadería:** Mayor parte de los artículos ofrecidos por la empresa comercializadora son de marcas extranjeras las cuales tienen la mejor calidad para ofrecer a la industria, sin embargo, la importación de estos productos suele demorar más de lo estimado debido a causas imputables a fábrica o la falta de cupos

para la importación por parte del transportista que afecta a la empresa debido a caer en incumplimiento de contratos y a su vez perder clientes.

### **3.3.4 Riesgos del Entorno**

- **Robo, hurto, fraude o asalto:** Los riesgos de hurto y fraude surgen por falencias en el control, dado que no se registra oportunamente en los sistemas de información, los bienes que ingresan y salen debido al descuido y desorganización por parte del responsable de ahí que se afecta al servicio entregado, ocasiona pérdidas económicas y la empresa se ve forzada a empezar investigaciones disciplinarias, fiscales, incluso penales. Los riesgos de robo y asalto se presentan debido al incremento de estos delitos en la sociedad ecuatoriana, lo cual va ligado a un problema social y está afectando a todo tipo de negocios.

- **Desastres naturales:** Los daños causados por catástrofes naturales como o terremotos, inundaciones e incendios se generan en el momento en el que ocurre el acontecimiento, sin embargo, estas catástrofes pueden generarse de manera inesperada, ya que son resultantes de procesos naturales y pueden traer a la empresa consecuencias negativas que implican pérdidas económicas, humanas, daños de infraestructura y reducción drástica de la operatividad.

### **3.3.5 Riesgos Ocupacionales**

- **Malentendidos y conflictos laborales:** Este tipo de riesgos se origina por la falta de sanción a personal que genera conflictos de manera recurrente, debido a que el liderazgo es deficiente no hay una correcta comunicación entre áreas, además existe oposición al cambio por parte de los empleados.

### 3.4 Análisis del riesgo inherente

Para poder calificar los riesgos inherentes que se presentan en la empresa, se procedió a establecer un valor del puntaje para medir el nivel de riesgo que fue determinado por la empresa según los indicadores detallados en la sección 2.4

**Tabla 8**

*Valoración del riesgo inherente*

Nº	Riesgos	Impacto	Probabilidad	Calificación	Nivel de Riesgo
1	Imposibilidad de vender a entidades públicas por incumplimiento de contratos.	5	2	10	Medio
2	Pérdida financiera por fuga de clientes	3	2	6	Medio
3	Incobrabilidad de cuentas	4	3	12	Alto
4	Concesión créditos a clientes con baja capacidad de pago.	3	3	9	Medio
5	Caída de los sistemas informáticos.	5	3	15	Alto
6	Rotura de stock	4	4	16	Alto
7	Retraso en la importación de la mercadería	4	4	16	Alto
8	Robo, hurto, fraude o asalto	4	3	12	Alto
9	Desastres naturales	5	1	5	Medio
10	Malentendidos y conflictos laborales.	3	3	9	Medio

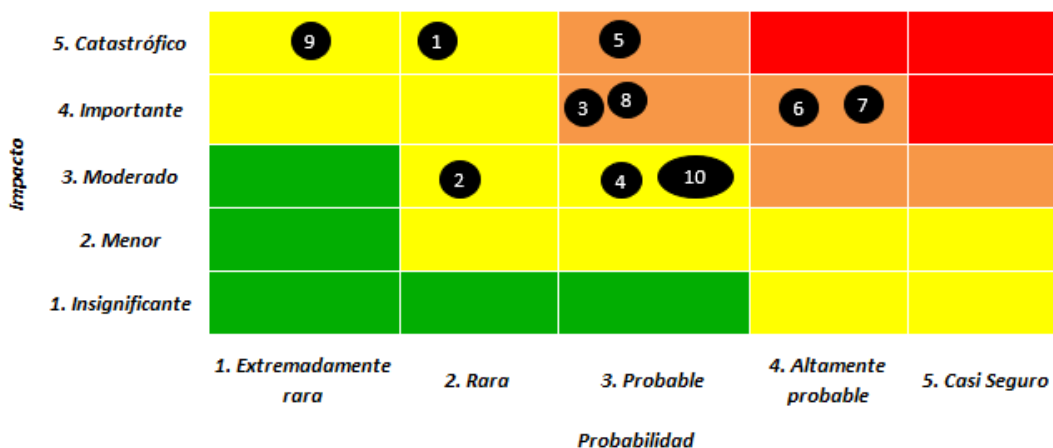
Fuente: Empresa Comercial de equipos industriales

En la tabla 8 se puede identificar la valoración cualitativa de los 10 riesgos que enfrenta la organización antes de implementar algún control o medida de mitigación, de los cuales aquellos como: Incobrabilidad de cuentas, caída de los sistemas informáticos, rotura de stock, el retraso en la importación de la mercadería, acciones como robo, hurto, fraude o asalto, mantienen una calificación de riesgo alto, cuyo nivel de impacto y probabilidad afectan significativamente las operaciones de la empresa.

Para mejor visualización del nivel de riesgo de acuerdo con su valoración, se elaboró el siguiente mapa de calor:

### Ilustración 6

#### Mapa de Calor Riesgo Inherente



*Fuente:* Elaboración propia

### 3.5 Calificación de Controles

De acuerdo con los criterios preestablecidos en el capítulo 2, evidencia, tipo, implementación y cumplimiento, se calculó el puntaje para cada uno de los controles determinados en la empresa comercializadora de equipos industriales en relación al riesgo neto de la empresa.

**Tabla 9***Valoración del control*

<b>Riesgos</b>	<b>Control</b>	<b>Resultado</b>	<b>Calificación</b>	<b>Resultado Control</b>
Imposibilidad de vender a entidades públicas por incumplimiento de contratos	Revisión de los documentos que se presentan a procesos públicos para validar el cumplimiento de todos los requisitos	37	2	Bajo
Pérdida financiera por fuga de clientes	No existe control	0	1	Muy bajo
Incobrabilidad de cuentas	Análisis crediticio completo. Concesión de créditos previo análisis documental.	64,5	4	Fuerte
Concesión de créditos a clientes con baja capacidad de pago	Validación de documentos soporte.	37	2	Bajo
Caída de los sistemas informáticos	No existe control	0	1	Muy bajo
Rotura de Stock	No existe control	0	1	Muy bajo
Retraso en el embarque de la mercadería	Gestionar la incidencia con el cliente ofreciendo opciones.	62,5	4	Fuerte
Robo, hurto, fraude o asalto	Contratación de mayor seguridad física y cámaras de video vigilancia	37	2	Bajo

Desastres naturales	Contratación de seguros	37	2	Bajo
Malentendidos y conflictos laborales.	Actividades de socialización para mejorar el ambiente laboral: cumpleaños, eventos especiales por festividades, etc. Canalización de quejas y reclamos mediante la Coordinación de Desarrollo Humano.	37	2	Bajo

*Fuente:* Elaboración propia

Se aprecia en la tabla, todos los controles relacionados a las amenazas que se enfrenta la organización de manera imprevista. Los controles establecidos en la tabla fueron adaptados por la organización según su necesidad y requerimientos, de los cuales se pudo determinar su calificación cualitativa según los criterios predeterminados. Controles como pérdida financiera por fuga de clientes, caída de los sistemas informáticos y rotura de stock mantienen un resultado de “Muy Bajo” que podría afectar el funcionamiento ininterrumpido de las actividades de la entidad, esto se debe a que la empresa no ha establecido controles para aquellos riesgos y su calificación es igual a 1, por lo que se establecen propuestas de controles para los mismos.

### ***3.5.1 Propuesta de Controles, para riesgos con calificación 0***

Para aquellos casos en los que no se haya establecido un control para el riesgo en la tabla de calificaciones su resultado será un valor igual a 1 y se establecerá una propuesta de control para una adecuada gestión, como se muestra en la tabla 10, simulando la implementación previa de los controles propuestos en la empresa.



**Tabla 10***Propuesta de controles*

<b>Riesgos</b>	<b>Nuevo Control</b>	<b>Resultado</b>	<b>Calificación</b>	<b>Resultado Control</b>
Pérdida financiera por fuga de clientes	Análisis de Satisfacción al cliente/ Encuestas de salida	62.5	4	Fuerte
Caída de los sistemas informáticos.	Actualización periódica y parches de seguridad/ Monitoreo continuo	37	2	Bajo
Rotura de stock	Pronósticos de demanda de inventario  Proveedor de respuesta rápida	37	2	Bajo

*Fuente:* Elaboración propia

### **3.6 Riesgo Residual**

Para la obtención de la calificación del riesgo residual se relaciona el nivel de riesgo natural y la ponderación de los controles para las 10 vulnerabilidades detectadas, con el fin de relacionar ambos elementos y determinar la magnitud del riesgo que permanece tras la aplicación de los controles.

La siguiente tabla muestra la relación de ambas variables para cada riesgo seleccionado:

**Tabla 11***Valoración del Riesgo Residual*

<b>N°</b>	<b>Riesgos</b>	<b>Nivel de Riesgo Inherente</b>	<b>Resultado de control de Riesgo</b>	<b>Nivel del Riesgo Residual</b>
<b>1</b>	Imposibilidad de vender a entidades públicas por incumplimiento de contratos	Medio	Bajo	Medio
<b>2</b>	Pérdida financiera por fuga de clientes	Medio	Fuerte	Bajo
<b>3</b>	Incobrabilidad de cuentas	Alto	Fuerte	Medio
<b>4</b>	Concesión créditos a clientes con baja capacidad de pago	Medio	Bajo	Medio
<b>5</b>	Caída de los sistemas informáticos	Alto	Bajo	Alto
<b>6</b>	Rotura de stock	Alto	Bajo	Alto
<b>7</b>	Retraso en la importación de la mercadería	Alto	Fuerte	Medio
<b>8</b>	Robo, hurto, fraude o asalto	Alto	Bajo	Alto
<b>9</b>	Desastres naturales	Medio	Bajo	Medio
<b>10</b>	Malentendidos y conflictos laborales	Medio	Bajo	Medio

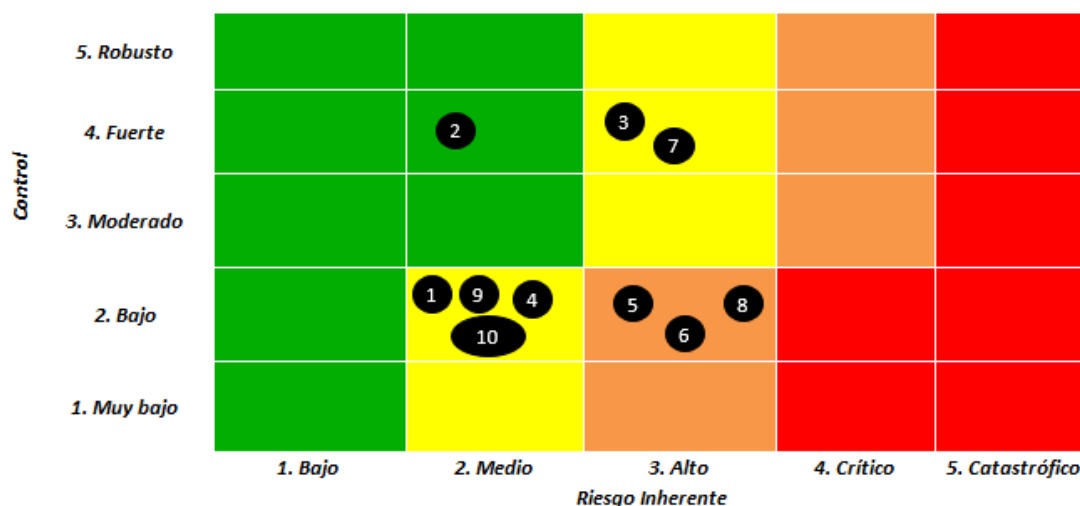
*Fuente:* Elaboración propia

Como resultado se identificó aquellas amenazas cuya magnitud es crítica después de haber aplicado las medidas de control o mitigación respectiva, tales como, la caída de los sistemas, la rotura de stock y el riesgo que ocurran hurtos, fraudes, robos y asaltos en la empresa, que de acuerdo con su nivel de riesgo existente representa una amenaza para la continuidad de las actividades que mantiene el establecimiento, por lo que se requiere implementar un plan de contingencia para mitigar el riesgo.

Para mejor visualización del nivel de riesgo residual de acuerdo con su valoración, se elaboró el siguiente mapa de calor:

### Ilustración 7

*Mapa de Calor Riesgo Residual*



*Fuente:* Elaboración propia

### 3.7 Estrategias y tratamiento

En la tabla 12 se detalló la respuesta a los riesgos seleccionados, que fue determinada en el cuadro de riesgos elaborado por la empresa, sin embargo, para aquellos que mantienen una criticidad “Alta” se procede a elaborar el plan de contingencia adecuado para su control.

**Tabla 12**

*Tratamiento por cada tipo de riesgo*

Riesgos	Respuesta al Riesgo	Tratamiento
Imposibilidad de vender a entidades públicas por incumplimiento.	Mitigar	Enfocar mayor parte de las ventas al sector privado

Pérdida financiera por fuga de clientes	Mitigar	Mejorar los procesos que se orientan a la fidelización.
Incobrabilidad de cuentas	Mitigar	Firma de pagaré para todos los clientes, obligatorio en personas naturales y en personas jurídicas se disminuye el cupo crediticio en caso de que no firmen el pagaré.
Concesión créditos a clientes con baja capacidad de pago.	Mitigar	Establecer criterios estrictos para la concesión de créditos
Caída de los sistemas informáticos.	Evitar	Plan de contingencia
Rotura de stock	Mitigar	Plan de contingencia
Retraso en la importación de la mercadería	Mitigar	Reforzar coordinación con fábrica para evitar retrasos.
Robo, hurto, fraude o asalto	Evitar	Plan de contingencia
Desastres naturales	Evitar	Contrato de seguros y evaluación de infraestructura.
Malentendidos y conflictos laborales.	Mitigar	Programas que incentiven la integración entre los colaboradores

*Fuente:* Elaboración propia

### 3.8 Planes de Acción

Se propuso acciones preventivas para cada riesgo crítico identificado en la empresa, para mostrar de forma clara y específica las estrategias que se deben implementar para conseguir los objetivos de la compañía, a continuación, se detalla la acción, el responsable, el tiempo y los recursos relacionados:

### 3.8.1 Plan de acción 1: Caída de los sistemas informáticos

**Tabla 13**

*Plan de acción del riesgo 1*

<b>Acciones</b>	<b>Fecha límite del plan de acción</b>	<b>Responsables</b>	<b>Recursos</b>
Monitoreo continuo para detectar problemas que ocasionen una futura caída de sistemas	31/12/2024	Jefe TIC (Personal)	<ul style="list-style-type: none"> <li>• Recurso humano, como Personal TIC</li> <li>• Software que monitorea la conectividad</li> <li>• Herramienta que evalúe el rendimiento de las aplicaciones.</li> <li>• Aplicaciones de respuesta ante contingencia.</li> </ul>
Generar copias de seguridad relacionadas con las operaciones de cada área, la información recopilada que mantenga 3 meses de antigüedad será depurada	31/12/2024	Personal TIC	<ul style="list-style-type: none"> <li>• Servicio de guardado en la nube.</li> <li>• Servicio de copias de resguardo.</li> <li>• Dispositivos de almacenamiento físicos, como pendrive, discos, memorias.</li> <li>• Recurso humano, como Personal TIC</li> </ul>
Llevar a cabo pruebas preventivas en el hardware y software para identificar posibles fallas en el sistema	31/12/2024	Personal TIC	<ul style="list-style-type: none"> <li>• Recurso humano, como Personal TIC</li> <li>• Herramientas, aplicaciones que evalúen el rendimiento del software.</li> <li>• Mantenimiento de Hardware.</li> </ul>

### 3.8.2 Plan de acción 2: Rotura de stock

**Tabla 14**

*Plan de acción del riesgo 2*

<b>Acciones</b>	<b>Fecha límite de implementación</b>	<b>Responsables</b>	<b>Recursos</b>
-----------------	---------------------------------------	---------------------	-----------------

Notificación por parte del programa cuando uno o varios productos mantengan niveles bajos o críticos en stock.	31/12/2024	Personal Compras	<ul style="list-style-type: none"> <li>• Sistema Informático</li> <li>• Recurso Humano como personal de TIC</li> </ul>
Realizar auditorías de inventarios para actualizar los niveles de stock de ser necesario	30/06/2024	Asistente de auditoría	<ul style="list-style-type: none"> <li>• Recurso Humano como personal de auditoría</li> <li>• Herramientas físicas para el recuento de existencias</li> </ul>
Solicitar un informe a los abastecedores nacionales para conocer variaciones en la demanda de algún producto	30/06/2024	Personal de compras	<ul style="list-style-type: none"> <li>• Recurso Humano como el personal de abastecimiento</li> <li>• Herramientas para la comunicación como laptop o teléfonos</li> </ul>
Establecer políticas con los proveedores y clientes para mejorar los acuerdos de suministro y tiempos de entrega.	31/03/2024	Coordinador de Calidad Gerente de Cadena de Abastecimiento	<ul style="list-style-type: none"> <li>• Recurso Humano como el personal de abastecimiento y personal de calidad</li> <li>• Inventario actualizado</li> </ul>
Actualizar los niveles máximos y mínimos en el inventario de los productos	29/02/2024	Personal de logística	<ul style="list-style-type: none"> <li>• Sistema informático</li> <li>• Productos físicos para el conteo</li> <li>• Recurso Humano como el personal de logística</li> </ul>

### 3.8.3 Plan de Acción 3: Hurto, fraude, robo, asalto o ataques de extorsión

Por solicitud de la empresa se consideraron planes de acción relacionados al riesgo de ataques de extorsión debido a que por su naturaleza es un evento crítico vinculado a robos.

**Tabla 15***Plan de acción del riesgo 3*

<b>Acciones</b>	<b>Fecha límite del plan de acción</b>	<b>Responsables</b>	<b>Recursos</b>
Capacitaciones semestrales al personal sobre cómo como identificar y manejar situaciones de extorsión o terrorismo, asaltos, entre otras emergencias.	30/06/2024	Personal SSO	<ul style="list-style-type: none"> <li>• Recurso humano como personal de Seguridad y Salud ocupacional</li> <li>• Herramientas como botiquín de primeros auxilios</li> </ul>
Evaluar y reforzar el control de acceso a las instalaciones y en áreas sensibles	31/12/2024	Personal SSO	<ul style="list-style-type: none"> <li>• Herramientas físicas como radios de comunicación, tolete, armas de fuego.</li> <li>• Recurso humano como guardias de seguridad</li> </ul>
Actualizar documentación soporte, como números telefónicos de personal clave para la gestión del riesgo y personal de alta vulnerabilidad.	30/06/2024	Personal Recursos Humanos	<ul style="list-style-type: none"> <li>• Personal de Recursos Humanos</li> <li>• Documentación física o digital con los números registrados</li> </ul>
Revisión de cámaras de vigilancias para detectar puntos ciegos dentro de las instalaciones, y emitir informe al comité.	29/02/2024	Personal SSO	<ul style="list-style-type: none"> <li>• Cámaras de seguridad</li> <li>• Monitores de vigilancia</li> <li>• Recurso humano como guardias de seguridad</li> </ul>

**3.9 Análisis de Costos y Beneficios**

Se procedió a analizar e identificar los costos estimados en la creación del manual para gestión de contingencias de la entidad comercializadora de equipos industriales, a través de un

modelo económicamente viable. Además, se cuantificó los beneficios que ofrece la implementación del manual en la empresa.

### 3.9.1 Valoración de Costos

A través de una tabla se detallaron los costos aproximados asociados a la creación del manual, con el fin de justificar los recursos implementados y determinar el valor que aporta el esfuerzo implementado.

**Tabla 16**

*Costos*

<b>Descripción</b>	<b>Cantidad</b>	<b>Precio Unitario</b>	<b>Valor Total</b>	<b>Descripción</b>
Movilización	8	\$5,00	\$40,00	Dinero utilizado para transporte ida y venida de la empresa.
Periférico de almacenamiento	1	\$11,00	\$11,00	Compra de un pendrive para almacenamiento de información
Horas trabajadas	290	\$12,00	\$3.480,00	Horas empleadas para el desarrollo del manual por el valor de consultoría por hora.
<b>Total</b>			<b>\$3.531,00</b>	

*Fuente: Elaboración propia*



### 3.9.2 Valoración de Beneficios

A través de la tabla se muestran los beneficios aproximados asociados al desarrollo del manual, con el objeto de evaluar el rendimiento financiero y operativo de la empresa una vez que se haya implementado, garantizando la maximización de recursos.

Beneficios monetarios

<b>Beneficio</b>	<b>Detalle</b>	<b>Valor inicial</b>	<b>Valor luego de implementar el manual</b>
Reducción de pérdidas monetarias	Caída de los sistemas	\$ 819.853,05	\$109.313,74
	Rotura de Stock	\$2.668.101,35	\$1.334.050,68
	Robo, Hurto, Fraude, Asalto	\$ 175.000,00	\$ 52.000,00
	<b>Total</b>	<b>\$3.662.954,41</b>	<b>\$1.495.364,42</b>

*Fuente: Elaboración propia*

**Tabla 17**

*Otros beneficios*

<b>Beneficio</b>	<b>Detalle</b>	<b>Cálculo</b>	<b>Valor luego de implementar el manual</b>
Mitigación de Riesgos Significativos	Riesgos residuales con relevancia máxima, sin considerar la propuesta de controles	Inicialmente existían 5 riesgos con criticidad considerable, luego de la implementación del manual 3 riesgos altos pasaron a criticidad media.	2 riesgos
Optimización de tiempo de respuesta ante contingencias.	Caída de los sistemas	Antes el tiempo de respuesta aproximadamente era de 5 días, luego de la implementación del manual se reducen 3 días de respuesta	2 días
	Rotura de Stock	Antes el tiempo de respuesta aproximadamente	3 días

---

	era de 7 días, luego de la implementación del manual se reducen 4 días de respuesta	
Robo, Fraude, Hurto, Asalto	Antes el tiempo de respuesta aproximadamente era de 3 días, luego de la implementación del manual se reduce a 1 día de respuesta	2 días

---

*Fuente: Elaboración propia*

Por lo tanto, estimando el valor de beneficio neto, considerando los beneficios monetarios una vez implementado el manual y reduciendo sus costos, obtenemos que:

**Beneficio Neto:** Total de Beneficio monetarios - Total de Costos

**Beneficio Neto:** (\$3.662.954,41 - \$1.495.364,42) - \$3.531,00

**Beneficio Neto:** \$ 2.167.589,99

## Capítulo 4

## 4. Conclusiones y Recomendaciones

### 4.1 Conclusiones

- I. El enfoque aplicado, mediante la obtención de información de la entidad y la calificación de riesgos y controles, permite identificar con precisión el nivel de riesgo que la empresa debe mitigar mediante medidas más estrictas. Esto se logra a través del desarrollo y ejecución de planes de acción específicos para cada riesgo.
- II. El diseño de este manual ayuda a los colaboradores de la empresa conocer con exactitud sus funciones y roles durante contingencias. Esto permite que la empresa responda de manera más rápida y efectiva, minimizando el impacto de la contingencia.
- III. La identificación de las amenazas más graves en la empresa permite enfocar un análisis adecuado para determinar las medidas necesarias a implementar con el fin de que el periodo de interrupción sea mínimo y no afecte en la continuidad las actividades de la organización.
- IV. Un plan de manejo de crisis permite gestionar con mayor eficiencia los riesgos identificados, desde la detección mínima del riesgo hasta el retorno de las operaciones de la empresa luego de una contingencia. Este plan se compone de tres etapas: prevención, contingencia y recuperación.
- V. El diseño de planes de contingencias a través de flujogramas permite entender mejor las acciones por cada riesgo categorizado de nivel alto y que de materializarse ocasionarían la interrupción en las operaciones de los procesos críticos.
- VI. Es importante contar con un directorio de continuidad para que la empresa mantenga contacto con entidades externas que aporten con sus servicios durante la ocurrencia de eventos emergentes en la empresa o a nivel macro en la ciudad.

## 4.2 Recomendaciones

- I. Para el buen uso de la herramienta diseñada se recomienda actualizar periódicamente el manual de procesos para gestión de contingencias. Esto se debe realizar una vez que se hayan llevado a cabo pruebas relacionadas a las acciones propuestas y se hayan determinado los lineamientos que pueden mejorarse en beneficio al personal, bienes e infraestructura de la compañía.
- II. Para gestionar con mayor eficiencia los riesgos críticos detectados en la organización y detectar nuevas amenazas, se recomienda organizar reuniones mensuales entre el Comité de Emergencias y los encargados de cada departamento.
- III. Elaborar un programa de capacitaciones mensuales relacionadas con los riesgos más importantes de la empresa y otorgar incentivos anuales a los colaboradores que cumplan con la asistencia a todas las capacitaciones, con el objetivo de brindar nuevos conocimientos y promover la integración departamental.
- IV. Evaluación y monitoreo trimestral de los riesgos y controles a implementar en la organización para actualizaciones de acuerdo a la demanda o exigencias recientes de la empresa.
- V. Fortalecer los controles preventivos de los riesgos que pueden pasar de criticidad media a alta, lo cual reducirá la posibilidad de una futura contingencia y permitirá administrar correctamente los recursos y disminuir costos a la compañía.

## 5. Referencias

International Organization for Standardization. (2019). *ISO 22301:2019 Guía de implantación*.

Obtenido de <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf>

Abdullah, A. M. (diciembre - enero de 2017 ). Evolution of Enterprise Resource Planning. *Excel*

*Journal of Engineering Technology and Management Science*(11), 6. Obtenido de <https://farapaper.com/wp-content/uploads/2018/08/Evolution-of-Enterprise-Resource-Planning.pdf>

Acosta Vega, R. K., Ospino Ayala, Ó. J., & Valencia Espejo , V. E. (enero - junio de 2017).

Diseño de un Sistema de Planificación de Recursos Empresariales (ERP) para una Microempresa. *INGE CUC*, 13(1), 84 -100.  
doi:<http://dx.doi.org/10.17981/ingecuc.13.1.2017.08>

Alarcón, G., Alarcón, P., & Guadalupe, S. (2019). La elaboración del mapa de procesos para una

universidad ecuatoriana. *Espacios*, 40(19), 4. Obtenido de <https://www.revistaespacios.com/a19v40n19/a19v40n19p04.pdf>

Alonso , C. (27 de septiembre de 2023). *Mapa de procesos de una organización, ¿qué es y cómo*

*se elabora?* . Obtenido de GlobalSuite Solutions:  
<https://www.globalsuitesolutions.com/es/que-es-mapa-de-procesos-y-como-se-elabora/>

Ambrosone, M. (2007). *La administración del Riesgo Empresarial: una responsabilidad de*

*todos-El Enfoque COSO*. PricewaterhouseCoopers. Obtenido de

[https://www.academia.edu/27991553/LA\\_ADMINISTRACION\\_DEL\\_RIESGO\\_EMPRESARIAL\\_UNA\\_RESPONSABILIDAD\\_DE\\_TODOS\\_EL\\_ENFOQUE\\_COSO](https://www.academia.edu/27991553/LA_ADMINISTRACION_DEL_RIESGO_EMPRESARIAL_UNA_RESPONSABILIDAD_DE_TODOS_EL_ENFOQUE_COSO)

Asanza Molina, M. I., Miranda Torres, M. M., Ortiz Zambrano, R. M., & Espín Martínez, J. A. (2016). Manual de procedimiento en la empresa. *Revista Caribeña de Ciencias Sociales*, 15. Obtenido de <https://www.eumed.net/rev/caribe/2016/11/manual.html>

Bravo Arias, C. B. (2022). *Herramienta Diagrama de Ishikawa para mejorar la Calidad de Servicio en el sistema de transporte público ferroviario, Lima 2022*. Obtenido de Universidad Norbert Wiener: [https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/7567/T061\\_77695897\\_T.pdf?sequence=1&isAllowed=y](https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/7567/T061_77695897_T.pdf?sequence=1&isAllowed=y)

Bueren, I. M., & Fiorentin, M. (abril de 2014). Influência de fatores contingenciais nos atributos do sistema de contabilidade gerencial: um estudo em empresas têxteis do estado do rio grande do sul. *Revista de Ciências da Administração*, 16(38), 196-212. Obtenido de <http://www.redalyc.org/articulo.oa?id=273530344014>

Contraloría General del Estado. (2023). *Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos*. Obtenido de Contraloría General del Estado: <https://www.contraloria.gob.ec/WFDescarga.aspx?id=1487&tipo=mul>

COSO. (2019). *COSO*. Obtenido de Asociación española para la Calidad: <https://www.aec.es/web/guest/centro-conocimiento/coso>

Departamento Nacional de Planeación. (2023). Manual de la Gestión de Continuidad del Negocio. 44. Obtenido de <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-PG-14%20Manual%20Gesti%C3%B3n%20de%20Continuidad%20del%20Negocio.Pu.pdf>

Dirección de Gestión y Desempeño Institucional. (noviembre de 2022). Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. *Función Pública*, 47 - 48. Obtenido de <https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%ABlicas+++Versi%C3%B3n+5+++Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=161124703>

Fustillos Parra, G. F. (julio de 2010). *Implementación de la unidad de contabilidad y diseños de procedimientos administrativos y contables en la empresa Mileno SC*. Obtenido de Universidad Politécnica Salesiana Sede Quito: <https://dspace.ups.edu.ec/bitstream/123456789/4408/1/UPS-QT01786.pdf>

Gómez Vargas, M., Galeano Higueta, C., & Jaramillo Muñoz, D. (julio-diciembre de 2015). El estado del arte; una metodología de investigación. *Revista Colombiana de Ciencias Sociales*, 6(2), 423 - 442. Obtenido de <https://www.redalyc.org/pdf/4978/497856275012.pdf>

Hernández Sampieri, R. (2014). Formulación de hipótesis. En R. Hernández Sampieri, C. Fernández Collado, & M. D. Baptista Lucio, *Metodología de la investigación* (Vol. 6, págs. 102 - 125). México: Mc Graw-Hill. Obtenido de <https://www.esup.edu.pe/wp->



content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-  
Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Iacub, P. (2015). Definición y marco histórico del software ERP. En P. Iacub, *Software ERP: El nuevo Gran Hermano de las organizaciones*. Buenos Aires, Argentina: Autores de Argentina. Obtenido de <https://bit.ly/3phEmbX>

International Organization for Standardization. (2018). *Norma Internacional ISO 31000:2018 Gestión del riesgo — Directrices*. Obtenido de ISO:  
[http://forestales.ujed.mx/succi/recursos/documento\\_29.pdf](http://forestales.ujed.mx/succi/recursos/documento_29.pdf)

Lavell, A. (2001). Apuntes para una reflexión institucional en países de la Subregión Andina sobre el enfoque de la Gestión del Riesgo. *Predecan*, 4, 1-22. Obtenido de [https://www.academia.edu/9808476/Sobre\\_la\\_Gesti%C3%B3n\\_del\\_Riesgo\\_Apuntes\\_hac%C3%ADa\\_una\\_Definici%C3%B3n](https://www.academia.edu/9808476/Sobre_la_Gesti%C3%B3n_del_Riesgo_Apuntes_hac%C3%ADa_una_Definici%C3%B3n)

López Serrazina, R., Jiménez Ayala, J., & Catató Alis, J. (5 de junio de 2023). Desarrollo y validación de un nuevo método de evaluación de riesgos eléctricos para la prevención y mitigación de daños a personas e instalaciones. *Ingeniare. Revista chilena de ingeniería*, 31(4), 15. doi:<https://dx.doi.org/10.4067/s0718-33052023000100204>

Madrid Nicolás, R., & Serrano Madrid, J. (2019). Matriz de riesgos. ¿En qué consiste, cómo se construye, cómo se gestiona? *Revista de Contabilidad y Dirección*(28), 57 - 68. Obtenido de [https://accid.org/wp-content/uploads/2020/08/RCD28\\_CAST-58-69-1.pdf](https://accid.org/wp-content/uploads/2020/08/RCD28_CAST-58-69-1.pdf)

Mora Horta , L. H. (13-14 de octubre de 2016). *Guía práctica -armado una precisa matriz de riesgos*. Obtenido de Asociación de Especialistas Certificados en Delitos Financieros:

[https://www.flexcompliance.com/repository/LUCIO\\_MORA\\_GUIA\\_PRACTICA\\_PARA\\_EL\\_ARMADO\\_DE\\_UNA\\_PRECISA\\_MATRIZ\\_DE\\_RIESGOS.pdf](https://www.flexcompliance.com/repository/LUCIO_MORA_GUIA_PRACTICA_PARA_EL_ARMADO_DE_UNA_PRECISA_MATRIZ_DE_RIESGOS.pdf)

Mora Lema, M. J. (2011). La teoría contingencial en la administración. *Cuadernos De Administración*, 6(7), 21 -32. doi:<https://doi.org/10.25100/cdea.v6i7.330>

Pardinas, F. (1989). *Metodología y técnicas de investigación en ciencias sociales*. Mexico: Siglo XXI. Obtenido de <https://books.google.com.ec/books?id=PDqKweTKbhUC&printsec=frontcover&hl=es#v=onepage&q&f=false>

Pico, G. (2006). El mapa de procesos: Elemento fundamental de un sistema de gestión de calidad para empresas de servicios en Venezuela. *Revista Venezolana de Análisis de Coyuntura*, XII(2), 291-309. Obtenido de <https://www.redalyc.org/articulo.oa?id=36412216>

Quincha Yumbla, G. J. (s.f.). *Diseño de un plan de emergencia y contingencia para la Empresa Galapesca S.A.* Obtenido de <https://repositorio.ug.edu.ec/items/c510b071-c744-4beb-822b-c269ba8e5f79>

Rodríguez Gallego, M. R., & Ordóñez Sierra, R. (septiembre - diciembre de 2012). MODELO DE GESTIÓN PARA LA CALIDAD EN LAS PRÁCTICAS DE PEDAGOGÍA. *Revista de Currículum y Formación de Profesorado*, 16(3), 357-372. Obtenido de <https://www.redalyc.org/pdf/567/56725002018.pdf>

Rodríguez López, M., Piñeiro Sánchez, C., & de Llano Monelos, P. (2013). Mapa de riesgos: Identificación y gestión de riesgos, *Atlantic Review of Economics*. *Atlantic Review of Economics*, 2. Obtenido de <https://www.econstor.eu/bitstream/10419/146556/1/776123106.pdf>

Romero Bermúdez, E., & Díaz Camacho, J. (2010). El uso del diagrama causa-efecto en el análisis de casos. *Revista Latinoamericana de Estudios Educativos (México)*, *XL*(3-4), 127-142. Obtenido de <https://www.redalyc.org/pdf/270/27018888005.pdf>

Westreicher, G. (1 de 6 de 2020). *Contingencia*. Obtenido de Economipedia: <https://economipedia.com/definiciones/contingencia.html>

Zetina-Bautista, E. d., Huicab-García, Y., & Coop-Abreu, R. E. (diciembre de 2021). Diseño de un manual de puestos para el Comité Ejecutivo SUTSET sección 16. *593 Digital Publisher CEIT*, *6*(6-1), 288-297. Obtenido de Digital Publisher CEIT: [https://www.593dp.com/index.php/593\\_Digital\\_Publisher/article/view/890/894](https://www.593dp.com/index.php/593_Digital_Publisher/article/view/890/894)

## **ANEXO 1**

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>1</b> de <b>35</b>
---	---	------------------------------

**MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS**  
**EMPRESA DE COMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES**

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 2 de 35
---	---	----------------

## INDICE

1	Introducción.....	4
2	Objetivo .....	4
3	Alcance .....	5
4	Glosario .....	5
5	Políticas relativas al manual .....	7
6	Etapas .....	7
6.1	Análisis de Riesgos.....	10
6.1.1	Identificación de bienes y personas susceptibles a un daño:.....	10
6.1.2	Contingencias .....	11
6.1.3	Responsables. ....	12
6.2	Partes interesadas para la continuidad del negocio .....	13
6.3	Tipo de Riesgo.....	14
6.3.1	Operativos y de Gestión .....	14
6.3.1.1	Riesgo: Caída de los Sistemas Informáticos .....	14
6.3.1.1.1	Definición de Equipo de Gestión.....	14
6.3.1.1.2	Comunicaciones en Crisis.....	14
6.3.1.1.3	Plan de manejo de crisis.....	15
6.3.1.2	Riesgo 2: Rotura de Stock.....	19
6.3.1.2.1	Definición de Equipo de Gestión.....	19
6.3.1.2.1	Comunicaciones en Crisis.....	19
6.3.1.2.2	Plan de manejo de crisis.....	20
6.3.2	Eventos Externos .....	25
6.3.2.1	Riesgo 3: Robo, Hurto, Fraude, Asalto o Ataques de Extorsión.....	25
6.3.2.1.1	Definición de Equipo de Gestión.....	25
6.3.2.1.2	Comunicaciones en Crisis.....	26
6.3.2.1.3	Plan de manejo de crisis.....	26
7	ANEXOS.....	34
7.1	Directorio de Continuidad .....	34
7.1.1	Contingencia 1: Caída del Sistema ERP .....	34
7.1.2	Contingencia 2: Rotura de Stock.....	34
7.1.3	Contingencia 3: Ataques de extorsión.....	34

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>3</b> de <b>35</b>
---	---	------------------------------

7.2    Números telefónicos de cooperativas de taxis.....35

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 4 de 35
---	---	----------------

## 1 Introducción

Hoy en día, la empresa de comercialización de equipos industriales vende e instala herramientas de bombeo de fluidos para diversas actividades y sectores productivos del país, cuya finalidad principal se enfoca en cumplir los requerimientos del mercado a través de producto y asesorías de calidad hacia los clientes, mejorando la utilización de recursos y generando ventajas tanto para sus empresas como para el mercado ecuatoriano.

En la estructura organizativa actual, los departamentos de Crédito y Cobranzas, Logística y Comercial son esenciales para el progreso y la continuidad de las operaciones. Debido al rol fundamental que desempeñan estos departamentos se ven expuestos a enfrentar riesgos significativos durante el desarrollo de sus operaciones, ya sea a nivel interno o externo, es por esto que, la empresa requiere de un registro directrices que permitan gestionar eficazmente las contingencias más comunes a presentar.

El diseño del manual fortalece la preparación de la empresa frente a eventos imprevistos, contribuyendo a la eficiencia operativa, la seguridad del personal y el resguardo de los bienes de la entidad, a través de la implementación de una serie de pasos y procedimientos a seguir para mantener el orden de las operaciones y el personal involucrado. Este enfoque sistemático reducirá el tiempo de reacción y mitigará el impacto negativo en las operaciones, además fortalecerá la resiliencia de la organización y respaldará su compromiso constante con la eficiencia y la satisfacción del cliente.

## 2 Objetivo

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial



EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 5 de 35
---	---	----------------

Establecer las directrices a seguir en los casos de materialización de los riesgos en procesos significativos con el fin de minimizar el impacto en las operaciones y continuar con las actividades.

### 3 Alcance

El manual de procesos para gestión de contingencias describe y abarca los procesos y actividades relacionadas a los departamentos de Crédito y Cobranzas, Logística y Abastecimiento y Comercial de la empresa, para identificar posibles impactos negativos durante la ocurrencia de eventos de desastre o interrupción mayor dirigido al personal, equipo y actividades. Estos riesgos que se presenten con una criticidad “Alta” serán evaluados según su nivel de crisis. El manual es de aplicación continua y será revisado y actualizado periódicamente para adaptarse a cambios en el entorno empresarial y garantizar su relevancia a lo largo del tiempo.

### 4 Glosario

- **Contingencias:** Es una situación futura e incierta que podría afectar significativamente a una organización o proyecto, ya sea de manera positiva o negativa, es decir, se trata de eventos no previstos que afectan funcionamiento, decisiones y resultados.
- **Mitigación:** La acción de disminuir o controlar el efecto de posibles amenazas mediante la aplicación de estrategias y acciones preventivas para reducir al mínimo la ocurrencia de eventos desfavorables o mitigar sus impactos negativos.
- **Prevención:** Previsión o intervención anticipada con el propósito de prevenir la aparición de eventos indeseados o posibles problemas,

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 6 de 35
---	---	----------------

mediante la aplicación de medidas y estrategias preventivas, con el fin de reducir la posibilidad de que se materialicen situaciones adversas.

- **Tiempo de recuperación:** El lapso requerido para restablecer un sistema o procedimiento a su condición operativa habitual tras enfrentar una interrupción o incidente imprevisto. Durante este período, la empresa debe planificar y aplicar acciones que posibiliten la recuperación eficaz de las funciones esenciales de la organización.
- **Plan de acción:** Un documento estratégico que describe acciones concretas para lograr metas predeterminadas, como la continuidad del negocio. Este documento establece de manera clara y precisa las tareas, recursos y plazos, evitando la interrupción de operaciones.
- **Gestión de continuidad del negocio:** Habilidad de una organización para preservar sus operaciones fundamentales y funciones críticas en situaciones adversas e imprevistas, garantizando su resiliencia ante tales escenarios.
- **Sistemas informáticos:** Son conjuntos interconectados de hardware, software y redes planificados para la retención y transmisión de datos en una organización, facilitando estas funciones mediante la utilización de aplicaciones especializadas en la realización de tareas específicas.
- **Emergencia:** Una circunstancia crítica que requiere una respuesta inmediata para su recuperación y la reducción de sus impactos negativos. Las emergencias engloban situaciones tales como desastres naturales, actos de terrorismo, crisis sanitarias y otros tipos de accidentes.

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 7 de 35
---	---	----------------

- **Extorsión:** Acción criminal que involucra amenazas o eventos violentos con el propósito de presionar a la víctima para obtener algo de valor.

## 5 Políticas relativas al manual

- Este manual de procesos para gestión de contingencias deberá cubrir aquellos procedimientos críticos, recursos e infraestructura de la compañía, de acuerdo con los bienes y servicios a ofrecer.
- Este manual deberá revisarse y actualizarse de forma periódica, acorde a los cambios de la entidad.
- El personal involucrado en el manual será acorde al riesgo y proceso en relación, y será comunicado por la alta gerencia para su respectiva ejecución.

## 6 Etapas

Para el desarrollo del manual se establecieron las siguientes etapas a seguir por cada riesgo crítico identificado en la organización:

- **Análisis de Riesgos:** Se lleva a cabo la detección, examen y valoración de los riesgos importantes que podrían resultar en repercusiones adversas para el desempeño de las operaciones de la compañía.
- **Identificación de partes interesadas:** Se reconoce todas las personas interesadas y sus necesidades en el manejo de contingencias por parte de la empresa, para tener conocimiento si pueden verse afectados de alguna forma. Además, de corroborar el compromiso de todos durante un evento imprevisto.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

- **Tipo de riesgo:** Se define el tipo de riesgo de acuerdo con el área o proceso relacionado, ya sea operativo y de gestión o por eventos externos, para así establecer de forma clara los siguientes puntos para su mitigación:
- **Definición del Equipo de gestión de riesgos:** Se designa de forma jerárquica a los líderes y personal de apoyo para gestionar los riesgos asociados a un proceso, así como las responsabilidades a desarrollarse para implementar las acciones descritas en los planes.

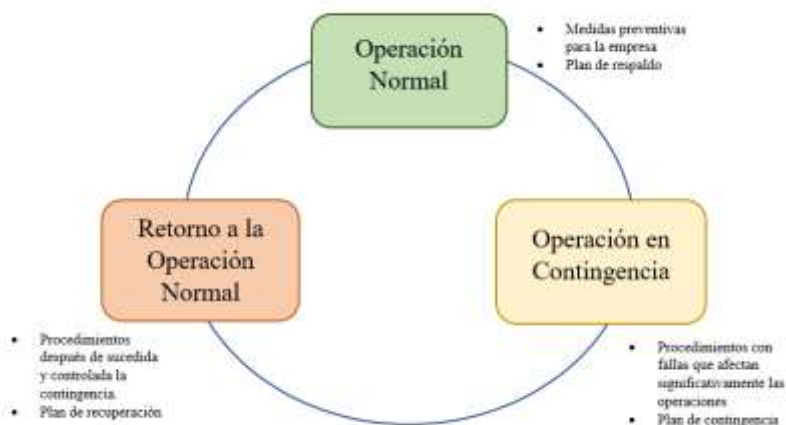


**Fuente:** Departamento Nacional de Planeación (2023).

- **Comunicación interna y externa:** Se realiza un análisis de las partes que componen la organización, a quienes se les debe comunicar las situaciones de contingencia

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

- **Plan de manejo de crisis:** Se detallan medidas y acciones para mitigar y controlar el riesgo antes, durante y después de su ocurrencia



**Fuente:** Departamento Nacional de Planeación. (2023).

- **Operación normal:** Se plantean medidas preventivas para evitar la materialización de la contingencia identificada y el grupo de responsables encargados para llevar a cabo el cumplimiento del plan.
- **Operación en contingencia:** En el caso de que un riesgo no pueda ser mitigado a través de las medidas preventivas establecidas en el proceso de operación normal, se debe establecer y poner en marcha la ejecución del plan de contingencias, mediante una serie de pasos a realizar durante situaciones emergentes, con el propósito de disminuir aquellos efectos desfavorables presenten en la organización. En el plan de contingencia se detallan los responsables y el personal de apoyo involucrado, así como el periodo en que inicia y finaliza el plan, los medios de comunicación y tiempo de máximo que la entidad puede tolerar la interrupción y recuperación de sus actividades.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>10</b> de <b>35</b>
---	---	-------------------------------

- Retorno a la operación normal: El plan de retorno o también conocido como plan de recuperación contiene estrategias para ayudar a la organización a recuperarse después de la ocurrencia de la contingencia y poder volver al curso normal de sus operaciones, tiene como objetivo disminuir el tiempo de inactividad, restaurar los procedimientos críticos y proteger los bienes susceptibles al daño. Dentro del plan de recuperación se describen los responsables de ejecutar las acciones de recuperación y las estrategias a emplear.

A continuación, se detallan las etapas por tipo de riesgo:

## **6.1 Análisis de Riesgos**

Se identificaron, evaluaron y priorizaron aquellos riesgos potenciales que podrían afectar significativamente a la empresa. Esta evaluación se realizó a partir del análisis de los riesgos residuales que la empresa mantiene con una criticidad alta luego de haber implementado controles preventivos y detectivos.

### **6.1.1 Identificación de bienes y personas susceptibles a un daño:**

Las personas que pueden ser afectadas por las contingencias posibles a presentarse son:

- Personal: Todos los colaboradores de la empresa, que lleva a cabo funciones específicas de acuerdo con su cargo.
- Clientes: Las personas que adquieren el producto, luego efectuarse una venta

Los bienes que pueden sufrir daños durante la materialización de los riesgos previamente contemplados son:

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>11</b> de <b>35</b>
---	---	-------------------------------

- **Sistemas Informáticos:** Infraestructura tecnológica y aplicaciones de software utilizadas para realizar tareas en la empresa y almacenar información relacionada a la misma.
- **Datos informáticos:** Información de la empresa digital almacenada y utilizada para la gestión y operaciones de equipos y productos industriales de la organización.
- **Documentación:** Registros, manuales, informes y procedimientos en físico que detallan operaciones relacionadas a la empresa y su naturaleza.
- **Productos industriales:** Productos comercializados por la empresa, para la generación de ventas e ingresos.
- **Bienes monetarios:** Activos financieros de la empresa, representados en dinero.
- **Equipos de la empresa:** Activos físicos y tecnológicos utilizados en las operaciones comerciales de la empresa.

### **6.1.2 Contingencias**

Las posibles contingencias que podrían materializarse aún después de haber implementado controles preventivos, por una inadecuada gestión son:

- **Caída de los sistemas informáticos:** La empresa comercial ha sufrido en dos ocasiones la caída de sus sistemas informáticos debido a la generación de códigos maliciosos, hackeos y delitos cibernéticos, que pueden ocasionar demoras en el servicio, interrupciones en las operaciones y a su vez pérdidas económicas a corto plazo, generando de esta forma molestia en sus clientes frecuentes.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 12 de 35
---	---	-----------------

- **Rotura de stock:** La empresa en ocasiones no cuenta con un volumen de inventarios suficientes para cumplir con las peticiones de los clientes, esto se debe a la interrupción en el suministro de materia prima y que en ocasiones el proveedor no dispone de stock del producto en el momento requerido.
- **Hurto, fraude, robo, asaltos o ataques de extorsión:** Los riesgos de hurto y fraude surgen por falencias en el control, dado que no se registra oportunamente en los sistemas de información, los bienes que ingresan y salen debido al descuido y desorganización por parte del responsable, ocasionando de esta forma pérdidas económicas en la empresa. De la misma forma los actos de robo, asalto y ataques de extorsión aparecen por el incremento de estos delitos en el país, lo cual va ligado a un problema social y está afectando a una diversidad negocios.

### 6.1.3 Responsables.

**Líderes:** Como responsables de coordinar y verificar la ejecución de las actividades en los planes de respaldo, acción y recuperación se encuentran principalmente el Gerente Corporativo, Gerente de Sucursal, Subgerente Corporativo, en conjunto con diversos jefes de departamentos donde se desarrollan las contingencias.

**Personal de apoyo:** Como parte del personal de apoyo al desarrollo de las responsabilidades planificadas para asegurar el flujo constante de las operaciones, se encuentran los colaboradores de cada área, ejerciendo con exactitud sus funciones preestablecidas.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial



## 6.2 Partes interesadas para la continuidad del negocio

Esta herramienta es de uso y estudio para las siguientes personas en mención, con la finalidad de gestionar la información detallada y ejecutar los planes de recuperación frente a diversos eventos adversos que se presenten en la organización.

Partes Interesadas	Necesidades
Gerente General	Obtener información detallada de los procesos y procedimientos a seguir durante una contingencia, basadas en los protocolos y estrategias predefinidos. Establecer canales de comunicación para asegurar el cumplimiento de las actividades durante un evento adverso.
Empleados	Conocer información clara y detallada de los procedimientos y pasos específicos que deben seguir como área durante situaciones de contingencias. Definición de roles y responsabilidades a seguir para asegurar la distribución efectiva de tareas, así mismo permite identificar posibles capacitaciones necesarias para una mejor gestión del proceso.
Proveedores	Obtener información detallada sobre la continuidad en la cadena de suministro que permita a su vez el flujo en las operaciones comerciales Definir plazos, acciones relacionadas a contratos y compromisos durante emergencias.
Clientes	Conocer si la empresa está preparada para seguir respondiendo a sus solicitudes en mercadería en un caso de interrupción en las actividades
Accionistas	Cumplimiento de expectativas sobre la capacidad de la empresa para gestionar eventos inesperados Conocer sobre los riesgos que ocasionen un impacto negativo en el ámbito financiero.
Estado	Cumplimiento legal y normativo

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

### 6.3 Tipo de Riesgo

De acuerdo con los procesos de la empresa los riesgos críticos identificados pueden catalogarse como: Operativos y de Gestión y eventos externos

#### 6.3.1 Operativos y de Gestión

Se considera como riesgos operativos y de gestión a aquellos que surgen de las operaciones diarias de la empresa, relacionados a decisiones y acciones estratégicas para su mitigación, ya que pueden afectar la competencia de la entidad para conseguir sus metas, como lo son: La caída de los sistemas ERP y la Rotura de Stock.

##### 6.3.1.1 Riesgo: Caída de los Sistemas Informáticos

###### 6.3.1.1.1 Definición de Equipo de Gestión

Miembro del equipo	Responsabilidades
<b>Líder:</b> Jefe de sistemas	Dirigir las acciones coordinadas para la gestión de crisis en los sistemas.
<b>Apoyo 1:</b> Analista de sistemas	Sincronizar las actividades con el personal operativo y verificación de la intermitencia de los sistemas.
<b>Apoyo 2:</b> Todas las áreas de la empresa	Monitoreo de los sistemas para comunicar al personal técnico el estado del mismo en las operaciones cotidianas de la empresa.

###### 6.3.1.1.2 Comunicaciones en Crisis

- **Comunicación interna:** La comunicación interna en la organización durante la contingencia de la caída de los sistemas informáticos se da entre el personal operativo de los departamentos, Crédito y Cobranzas, Logística y Abastecimiento, Seguridad Ocupacional y Comercial de la empresa, para el monitoreo continuo de las operaciones que se realizan en las aplicaciones asociadas al sistema.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

- **Comunicación externa:** Se establecerá comunicación con el proveedor de los sistemas para establecer una asistencia técnica especializada, diagnosticar y resolver rápidamente el problema que ha causado la caída del sistema de forma temporal.

#### 6.3.1.1.3 Plan de manejo de crisis

Cabe destacar que la Caída de los Sistemas Informáticos afecta principalmente al proceso de Ventas y Despacho, por lo tanto, para atender adecuadamente la contingencia se evaluará el nivel de riesgo, conforme a las siguientes consideraciones, con la finalidad de establecer el plan adecuado para su gestión.

Nivel de Crisis	Descripción	Impacto	Recomendación
Nivel 1	Interrupciones menores en el sistema.	Retrasos en todos los procesos relacionados a la aplicación del sistema.	Confirmar la existencia de respaldo de información en nube. Si se soluciona el evento, se recomienda actualizar el plan de respaldo correspondiente, en caso contrario se escala al nivel 2.
Nivel 2	Interrupciones significativas en el sistema.	Pérdida de Ventas. Errores financieros y operativos.	Contactar al proveedor de servicios informáticos para aplicación de medidas correctivas inmediatas. Si se soluciona el evento, se recomienda actualizar el plan de respaldo correspondiente, en caso contrario se escala al nivel 3.
Nivel 3	Colapso total del sistema.	Eliminación total de la información de las operaciones. Pérdida de Ventas.	Se procede con la ejecución del plan de contingencia.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

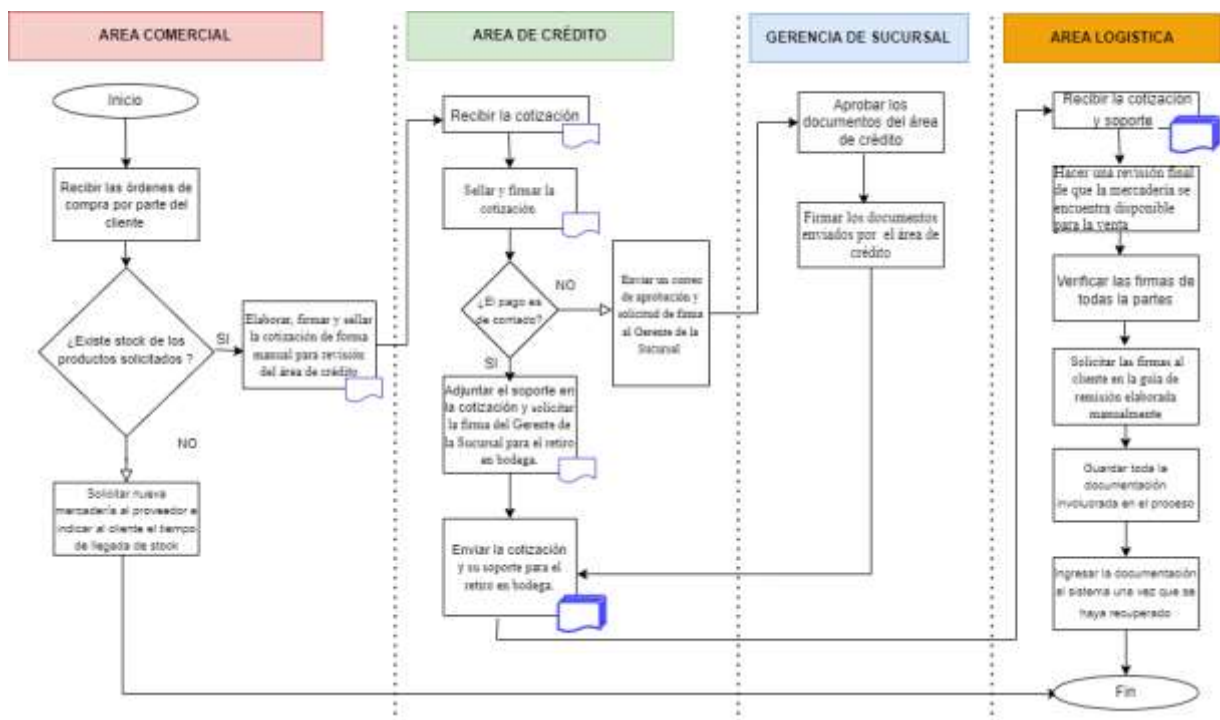
- **Plan de respaldo:** En esta sección se contemplan las medidas preventivas por interrupciones menores y significativas en el sistema. El propósito de este plan es evitar que se materialice esta contingencia.
  - Medidas Preventivas: Las medidas preventivas para la Intermitencia en el sistema son:
    - Jefe de sistemas: Realizar mantenimientos preventivos del sistema ERP
    - Personal operativo: Realizar diariamente respaldo de la información ligada a sus operaciones, en nube y en disco físico.
- **Plan de Contingencia:** Si la contingencia escala al nivel 3 de acuerdo con los niveles de crisis, se produce el colapso total de los sistemas en la empresa y se debe proceder a la ejecución del siguiente plan:
  - Descripción de actividades

Actividad	Responsable
Reportar a su superior o al encargado del área de TIC el problema de la interrupción de los sistemas.	Personal que detecte la caída del sistema
Recibir las órdenes de compra por parte del cliente, se confirma la existencia de las cantidades solicitadas por el cliente, y que dicha mercadería no esté reservada para otro cliente	Personal comercial
Elaborar, firmar y sellar la cotización de forma manual para revisión del área de crédito	Personal comercial
Recibir la cotización y verificar si el cliente cuenta con crédito o si realizó el pago. Luego de la confirmación sella y firma la cotización	Gestor de crédito
Si el pago es de contado, se adjunta el soporte en la cotización y solicita la firma del Gerente de la Sucursal para el retiro en bodega.	Personal comercial
Si el pago es a crédito se envía un correo de aprobación y solicitud de firma por parte del Gerente de la Sucursal para luego enviar a bodega.	Personal comercial
Aprobar los documentos del área comercial.	Gerencia de sucursal

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

Recibir la cotización, realizar una última confirmación de que la mercadería no está reservada para otro cliente, verificar las firmas para continuar con el despacho y solicitar las firmas al cliente en la guía de remisión elaborada manualmente.	Personal de logística
Guardar el archivo consecutivo de las entregas, junto con los traslados entre bodegas – talleres y órdenes de compra recibidas para posterior ingreso en el sistema	Personal de logística

*Proceso: Ventas y Despacho*



○ Periodicidad:

La periodicidad del plan de contingencia debe ser realizado cada vez que se presenten intermitencias mayores en el sistema como el colapso del mismo.

○ Responsable:

Jefes de cada área afectada: Encargado Comercial, Encargado de Créditos y Cobranzas y Encargado de logística

○ Personal de apoyo:

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

Colaboradores de las áreas afectadas

- Inicio de la actividad

Momento que detecte la caída del sistema.

- Finalización de la actividad

Recuperación total del sistema.

- Canales de comunicación:

Durante la caída de los sistemas en la empresa la comunicación interna puede gestionarse eficazmente mediante canales como: Correo electrónico profesional para comunicados, notificaciones y decisiones de la directiva de la empresa que mantendrá informados a los colaboradores.

Además, como medio informal se puede utilizar la herramienta Microsoft Teams y WhatsApp para consultas y gestiones grupales.

- Tiempo de máximo que la empresa puede tolerar la interrupción de sus actividades y tiempo de recuperación:

Riesgo	Proceso Crítico	Tiempo máximo de interrupción (MTPD)	Tiempo aceptable para la reanudación de actividades (RTO)
Caída de los sistemas informáticos.	Ventas y Despacho	5 días	5 días

- **Plan de recuperación** Como plan de recuperación se consideran las siguientes acciones necesarias después de sucedida y controlada la caída de los sistemas, con la finalidad de restaurar el estado de los procesos tal y como se encontraban antes del acontecimiento de la contingencia.

- Actividades de Recuperación

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 19 de 35
---	---	-----------------

- Jefe de sistemas: Reactivación de sistemas informáticos
- Responsables de cada área afectada: Suministra información recopilada por las copias de seguridad durante la caída del sistema al área de TICs.
- Personal de sistemas: Actualiza en el sistema la información proporcionada por los responsables de área.

### 6.3.1.2 **Riesgo 2: Rotura de Stock**

#### 6.3.1.2.1 *Definición de Equipo de Gestión*

Miembro del equipo	Responsabilidades
<b>Líder:</b> Gerente de cadena de abastecimiento	Dirigir las acciones coordinadas para la gestión de crisis por poca existencia de productos en stock.
<b>Apoyo 1:</b> Coordinadores de Logística	Examinar el número de inventarios de la compañía y determinar la magnitud de la rotura de stock en términos de afectación al producto, compromisos de entrega y satisfacción al cliente, para comunicar al gerente de cadena de suministro el caso.
<b>Apoyo 2:</b> Analista de Abastecimiento	Levantar información con los encargados de logística para entender necesidades inmediatas y establecer prioridades en la adquisición de productos.

#### 6.3.1.2.1 *Comunicaciones en Crisis*

- **Comunicación interna:** La comunicación corporativa durante la contingencia de rotura de stock se debe establecer entre el departamento comercial y de logística con la finalidad de gestionar y verificar la cadena de suministros e informar dicho suceso a la directiva e implementar los planes de acción propuestos.
- **Comunicación externa:** Esta comunicación se establecería con los proveedores con los que se relacione la empresa, y también se considera a

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

los clientes para dar a conocer el producto sustituto a ofrecer en caso de fuerza mayor.

#### 6.3.1.2.2 Plan de manejo de crisis

Para atender adecuadamente la contingencia denominada Rotura de Stock se evaluará el nivel de riesgo, conforme a las siguientes consideraciones, con la finalidad de establecer el plan adecuado para su gestión.

Nivel de Crisis	Descripción	Impacto	Recomendación
Nivel 1	Rotura de stock de 1 a 10 productos.	<ul style="list-style-type: none"> <li>Insatisfacción por parte de los clientes.</li> </ul>	<ul style="list-style-type: none"> <li>Gestionar un posible sustituto del ítem desde el área comercial.</li> <li>Si se soluciona el evento, se recomienda actualizar el plan de respaldo correspondiente, en caso contrario se escala al nivel 2.</li> </ul>
Nivel 2	Rotura de stock de 11 a 50 productos en inventario.	<ul style="list-style-type: none"> <li>Insatisfacción por parte del cliente.</li> <li>Pérdida recurrente de ventas.</li> </ul>	<ul style="list-style-type: none"> <li>Indagar en las causas de la rotura de stock y aplicar tratamiento según análisis.</li> <li>Si se soluciona el evento, se recomienda actualizar el plan de respaldo correspondiente, en caso contrario se escala al nivel 3.</li> </ul>
Nivel 3	No mantiene más de 50 productos en inventario.	<ul style="list-style-type: none"> <li>Pérdida de ventas.</li> <li>Afectación en las ganancias de la empresa.</li> <li>Daño en la imagen corporativa</li> </ul>	<ul style="list-style-type: none"> <li>Se procede con la ejecución del plan de contingencia.</li> </ul>

- Plan de respaldo:** En esta sección se contemplan las medidas preventivas por la ausencia de productos en el inventario desde 1 a 50 ítems. El propósito de este plan es evitar que se materialice esta contingencia.

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial



EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>21</b> de <b>35</b>
---	---	-------------------------------

- Medidas Preventivas
  - Analista de abastecimiento: Monitoreo continuo del inventario, de forma mensual.
  - Analista de abastecimiento: Elaborar base de datos con proveedores nacionales de respaldo.
  - Personal comercial: Informar qué productos caen constantemente en riesgo de rotura de stock
- **Plan de Contingencia** Si la contingencia escala al nivel 3 de acuerdo con los niveles de crisis se produce la rotura de stock al no mantener más de 50 productos en inventario y se debe proceder a la ejecución del siguiente plan:
  - Descripción de actividades

Actividad	Responsable
El dpto. comercial comunica la rotura de stock al departamento de cadena de abastecimiento.	Personal comercial
Si el cliente no requiere el producto de forma urgente, se sigue el proceso normal de compra. Si el cliente requiere el producto de forma urgente se solicita 50% de anticipo y se realiza la compra a nivel local.	Personal comercial
Comunicarse de inmediato con los proveedores nacionales para verificar la disponibilidad y tiempos de entrega.	Analista de cadena de abastecimiento
El departamento de compra debe generar de manera urgente la solicitud de pedido correspondiente a los proveedores nacionales.	Analista de cadena de abastecimiento
El departamento comercial notificará al departamento de contabilidad sobre la necesidad urgente de realizar el pago al proveedor nacional.	Analista de cadena de abastecimiento

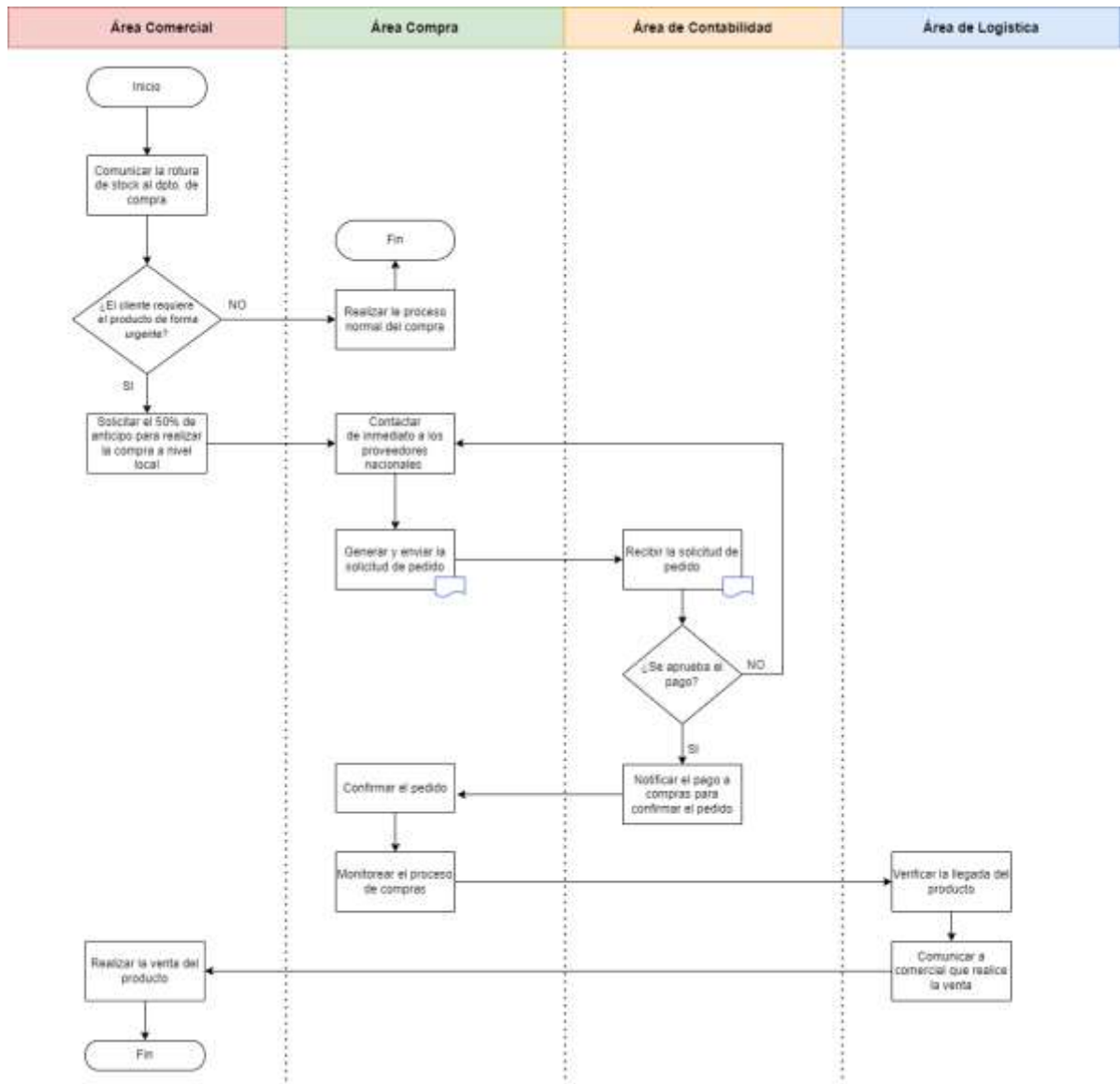
Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>22</b> de <b>35</b>
---	---	-------------------------------

El departamento de contabilidad aprobará el pago para evitar retrasos en la adquisición de productos.	Personal de contabilidad
Una vez aprobado el pago, el departamento de contabilidad notificará al departamento de compras para confirmar el pedido al proveedor nacional.	Personal de contabilidad
El departamento de compras deberá monitorear de cerca el proceso de entrega del proveedor nacional para asegurarse de que los productos lleguen a tiempo.	Analista de cadena de abastecimiento
Una vez que los productos lleguen y sean verificados por el departamento de logística, se actualizará el inventario.	Personal de logística
Comunicar al área comercial que realice la venta.	Personal de logística
Realizar la venta	Personal comercial

*Proceso: Comercial*

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial



- Periodicidad

La periodicidad del plan de contingencia debe ser realizada cada vez que se requiera realizar una venta urgente a un cliente importante y no exista stock para abastecerle.

- Responsable

El gerente de cadena de abastecimiento

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

- Personal de apoyo
  - Encargado de logística, encargado de adquisiciones.
- Inicio de la actividad
  - Momento en el que inicia la contingencia
- Finalización de la actividad
  - Cuando el inventario es actualizado y reabastecido.
- Canales de comunicación
  - Durante la contingencia de Rotura de Stock en la empresa la comunicación interna puede gestionarse eficazmente mediante canales como: Correo electrónico institucional para comunicados, notificaciones y decisiones de la directiva de la empresa que mantendrá informados a los colaboradores, Además, como medio informal se puede utilizar la herramienta Microsoft Teams y WhatsApp para consultas y gestiones grupales.
- Tiempo de máximo que la empresa puede tolerar la interrupción de sus actividades y tiempo de recuperación:

Riesgo	Proceso Crítico	Tiempo máximo de interrupción (MTPD)	Tiempo aceptable para la reanudación de actividades (RTO)
Rotura de stock	Comercial	7 días	5 días

- **Plan de recuperación:** Como plan de recuperación se contemplan las siguientes acciones necesarias después de sucedida y controlada la rotura de stock, cuya finalidad será restaurar el estado de las cosas tal y como se encontraban antes del acontecimiento de la misma

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>25</b> de <b>35</b>
---	---	-------------------------------

- Actividades de Recuperación
  - Analista comercial: Evaluar los productos más susceptibles a sufrir rotura de stock en el inventario.
  - Gerente de cadena de abastecimiento: Actualizar de forma periódica el plan mensual de compra del inventario.

### **6.3.2 Eventos Externos**

Se considera como riesgos de eventos externos a aquellos factores que provienen de situaciones fuera del control directo de la empresa y afectan considerablemente las operaciones, como lo es en el caso de que exista un robo, asalto, fraude o ataque de extorsión.

#### **6.3.2.1 Riesgo 3: Robo, Hurto, Fraude, Asalto o Ataques de Extorsión**

##### **6.3.2.1.1 Definición de Equipo de Gestión**

<b>Miembro del equipo</b>	<b>Responsabilidades</b>
<b>Líderes:</b> Gerente General, Subgerente Corporativo y Gerente de Sucursal	Dirigir coordinadamente las acciones y operaciones para salvaguardar a los trabajadores y bienes de la empresa.
<b>Apoyo 1:</b> Gerentes Comerciales	Coordinar comunicación con clientes y supervisar las medidas de seguridad en las transacciones comerciales
<b>Apoyo 2:</b> Coordinador de Recursos Humanos	Evaluará y proporcionará información de la persona involucrada de la empresa en caso de hurto o fraude y se comunicará directamente a los gerentes, de ser un fraude robo, asalto se comunicará directamente con entidades externas como la policía o personal de asesoría legal.
<b>Apoyo 3:</b> Jefe de Seguridad y Salud Ocupacional	Coordinar y ejecutar protocolos para proteger a los colaboradores y activos de la empresa, en conjunto a otros departamentos.

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página 26 de 35
---	---	-----------------

<b>Apoyo 4:</b> Jefe de TIC	Colaborar en la administración de la comunicación interna y externa asociada a la situación de emergencia.
<b>Apoyo 5:</b> Trabajadora Social	Llevar registro del estado y necesidades del personal y proporcionar seguimiento a largo plazo para garantizar el bienestar continuo.
<b>Apoyo 6:</b> Jefe de Marketing y Comunicación	Mantener a los empleados, proveedores, consumidores y demás partes involucradas sobre la situación.

Nota: Los miembros de este equipo pertenecen al Comité de Gestión de Emergencias

#### 6.3.2.1.2 Comunicaciones en Crisis

- **Comunicación interna:** Ante la eventualidad de un robo, hurto, fraude, asalto o extorsión en la organización, la comunicación interna se llevará a cabo a través del personal que identifique la contingencia. Dicha persona notificará de inmediato a su jefe de área, quien, a su vez, informará al Comité de Emergencias sobre la situación, quien se encargará de comunicar la contingencia a los empleados mediante el jefe de Seguridad y Salud Ocupacional.
- **Comunicación externa:** El personal de recursos humanos se comunicará con entidades policiales o un personal jurídico de ser el caso, de acuerdo con la magnitud del acto, para la respectiva gestión y toma de decisiones.

#### 6.3.2.1.3 Plan de manejo de crisis

Para atender adecuadamente la contingencia denominada Robo, Hurto, Fraude, Asalto o Ataques de extorsión se evaluará el nivel de riesgo, conforme a las siguientes consideraciones, con la finalidad de establecer el plan adecuado para su gestión.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

Nivel de Crisis	Descripción	Impacto	Recomendación
Nivel 1	Hurto, fraude, tentativa de robo.	<ul style="list-style-type: none"> <li>• Pérdidas financieras.</li> <li>• Desconfianza y afectación en la moral de los colaboradores.</li> <li>• Pérdida de bienes.</li> <li>• Afectaciones en el clima laboral.</li> </ul>	<ul style="list-style-type: none"> <li>• Revisión y monitoreo de la vigilancia en la empresa.</li> <li>• Si se soluciona el evento, se recomienda actualizar el plan de respaldo correspondiente, en caso contrario se escala al nivel 2.</li> </ul>
Nivel 2	Robo, Asalto	<ul style="list-style-type: none"> <li>• Pérdidas materiales.</li> <li>• Daños en infraestructura.</li> <li>• Interrupción de operaciones.</li> <li>• Miedo de los clientes y el personal.</li> <li>• Interrupción momentánea de las operaciones.</li> </ul>	<ul style="list-style-type: none"> <li>• Reforzar el personal de seguridad de la empresa.</li> <li>• Si se soluciona el evento, se recomienda actualizar el plan de respaldo correspondiente, en caso contrario se escala al nivel 3.</li> </ul>
Nivel 3	Actos de terrorismo, extorsiones.	<ul style="list-style-type: none"> <li>• Atentados contra la vida de las personas (clientes, colaboradores, visitantes).</li> <li>• Daños de alta magnitud a las instalaciones de la empresa.</li> <li>• Interrupción semi permanente de operaciones.</li> <li>• Pérdidas financieras cuantiosas.</li> <li>• Incremento de los gastos en seguridad.</li> </ul>	<ul style="list-style-type: none"> <li>• Se procede con la ejecución del plan de contingencia.</li> </ul>

- **Plan de respaldo**
  - **Nivel 1**

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>28</b> de <b>35</b>
---	---	-------------------------------

En esta sección se contemplan las medidas preventivas por el hurto, fraude y tentativa de robo con el propósito de evitar que se materialice esta contingencia.

- Medidas Preventivas

- Personal de Recursos Humanos: Realización de pruebas de polígrafo para la contratación de personal
- Personal de Seguridad Ocupacional: Capacitación de personal constante
- Personal Comercial: Realizar seguimiento de los productos vendidos y los artículos ingresados a bodega
- Auditor Interno: Realizar auditorías internas periódicas para identificar posibles irregularidades.
- Alta dirección: Restricción de personal a áreas críticas y confidenciales de la empresa.

- **Nivel 2**

Como medidas preventivas por robo y asalto. Se establecen las siguientes medidas para evitar que se materialice esta contingencia.

- Medidas Preventivas

- Jefe de Seguridad ocupacional: Contratación de un seguro de lucro cesante
- Jefe de sistemas: Reforzar sistemas de vigilancia, como cámaras de seguridad, en áreas clave dentro y alrededor de la empresa.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial



- Jefe de Seguridad ocupacional: Reforzar el personal de seguridad o utilizar servicios de seguridad privada para realizar patrullajes regulares.
  - Personal de mantenimiento: Mantener áreas alumbradas para alejar a potenciales intrusos.
  - Personal de Seguridad Ocupacional: Proporcionar entrenamiento regular sobre seguridad a los empleados y establecer planes de evacuación.
- **Plan de Contingencia.** Si la contingencia escala al nivel 3 de acuerdo con los niveles de crisis, se producen actos de terrorismo que dejan como consecuencia daños colaterales y se debe proceder a la ejecución del siguiente plan:
    - Descripción de actividades

Actividad	Responsable
Recibir la notificación de la llegada de una amenaza escrita o verbal a la empresa, por parte del jefe de área que identificó el riesgo.	Miembro del Comité de gestión de emergencias.
Notificar al personal la llegada de una amenaza escrita o verbal a las instalaciones, a través de las vías de comunicación establecidas.	Personal de Seguridad Ocupacional.
Avisar a la UNASE (Unidad Nacional de Antisecuestros y Extorsión) o a la Policía Nacional sobre la amenaza recibida.	Personal de Recursos Humanos
Comunicar al jefe de Seguridad y Salud Ocupacional la implementación de refuerzos en la seguridad.	Miembro del Comité de Emergencia
Implementar el refuerzo de la seguridad mediante la ubicación de guardias en puntos estratégicos de la empresa.	Jefe de Seguridad Ocupacional

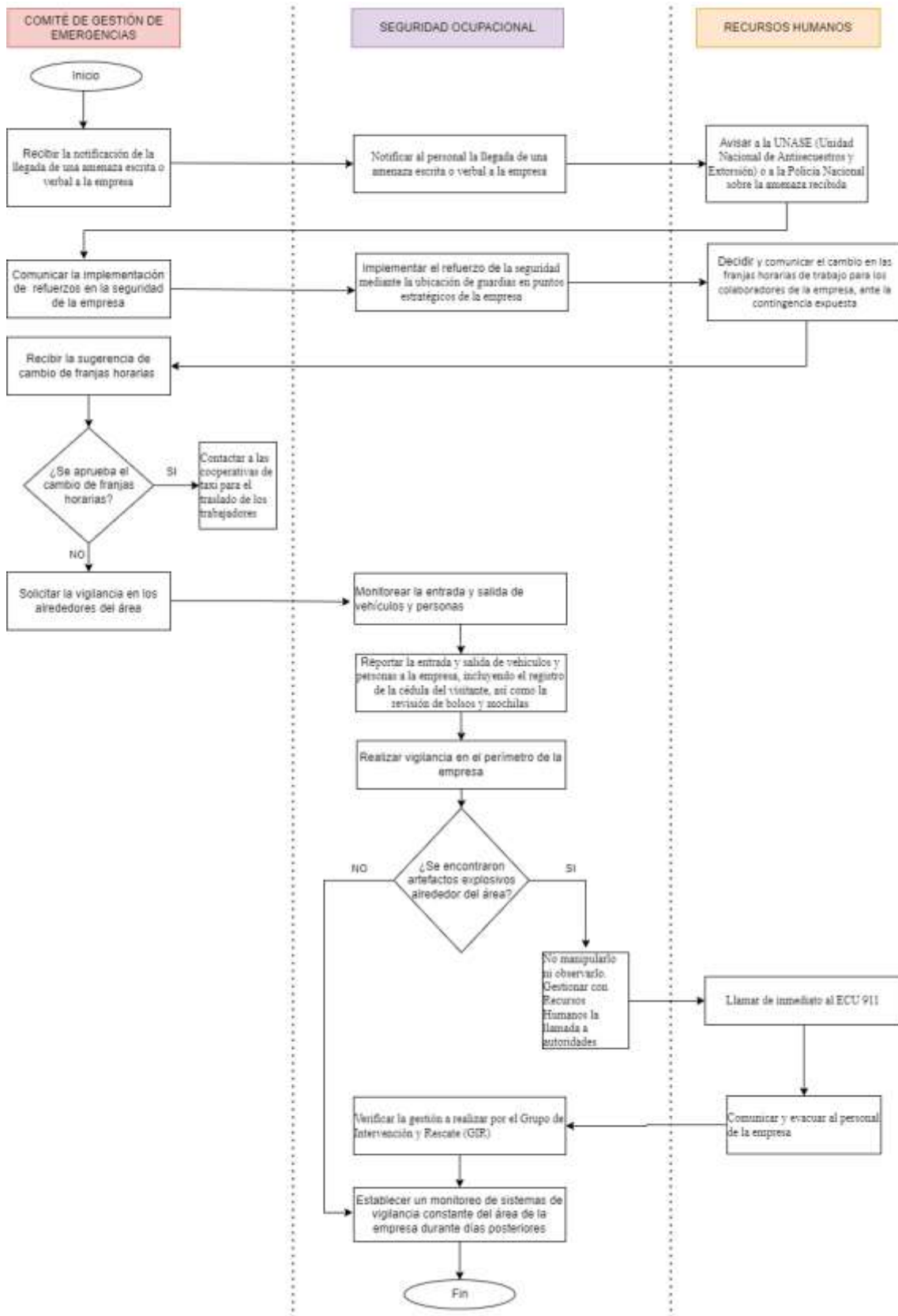
Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>30</b> de <b>35</b>
---	---	-------------------------------

Sugerir y comunicar el cambio de las franjas horarias de trabajo para los colaboradores de la empresa, ante la contingencia expuesta.	Jefe de Recursos Humanos
Si se aprueba el cambio se establecen las franjas horarias y se contacta a las cooperativas de taxi de confianza para el traslado de los trabajadores, si no se aprueba se continua con la vigilancia del perímetro.	Miembro del comité de Gestión de Emergencias
Monitorear el ingreso y partida de vehículos y personas a la empresa, al igual que la vigilancia de los alrededores del área	Personal de Seguridad Ocupacional
Reportar la entrada y salida de visitantes a la empresa, incluyendo el registro de la cédula, así como la revisión de bolsos y mochilas.	Personal de Seguridad Ocupacional
Identificar si existen ataques con artefactos explosivos, si existen no deben manipularlo ni observarlo detenidamente y comunicar al jefe de recursos humanos, en caso de que no existan artefactos solo se procede de forma preventiva un monitoreo constante del área de la empresa durante los días posteriores.	Personal de Seguridad Ocupacional
Llamar de inmediato al ECU911.	Jefe de Recursos Humanos
Comunicar al personal y evacuarlos del área que se encuentra en peligro	Personal de Recursos Humanos
Verificar la gestión a realizar por el GIR	Personal de Seguridad Ocupacional
Establecer un monitoreo de sistemas de vigilancia constante del área de la empresa durante días posteriores.	Personal de Seguridad Ocupacional

*Proceso: Actividades de administración*

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial



<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>32</b> de <b>35</b>
---	---	-------------------------------

- Periodicidad

La periodicidad del plan de contingencia debe ser realizado en los momentos en el que la empresa reciba un comunicado de amenaza por parte de una banda delictiva.

- Responsable

- Jefe de Seguridad Ocupacional
- Gerente de Sucursal

- Personal de apoyo

- Empresa de seguridad privada
- Personal de Seguridad Ocupacional

- Inicio de la actividad

Momento en el que inicia la contingencia

- Finalización de la actividad

Cuando los comunicados de amenazas cesen.

- Canales de comunicación

Durante ataques terroristas la comunicación interna puede gestionarse eficazmente mediante canales como: Correo electrónico institucional para comunicados, notificaciones y decisiones de la directiva de la empresa que mantendrá informados a los colaboradores.

A su vez se activará el correo de emergencias de la entidad con todos los integrantes del Comité de Gestión de Emergencias. A este correo se remitirá todas las comunicaciones oficiales.

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

Además, como medio informal se puede utilizar la herramienta Microsoft Teams y WhatsApp para consultas y gestiones grupales.

- Tiempo de máximo que la empresa puede tolerar la interrupción de sus actividades y tiempo de recuperación:

Riesgos	Proceso Crítico	Tiempo máximo de interrupción (MTPD)	Tiempo aceptable para la reanudación de actividades (RTO)
Actos de terrorismo, extorsiones.	Actividades de administración	2 días	5 días

- **Plan de recuperación.**

Como plan de recuperación se contemplan las siguientes acciones necesarias después de que cesen los actos de terrorismo que dejan como consecuencia daños colaterales, con la finalidad de restaurar el estado de las cosas tal y como se encontraban antes del acontecimiento de la misma:

- Gerente Financiero y Jefe de Seguridad y Salud Ocupacional:  
Determinar los impactos ocasionados por las extorsiones y gastos por servicios de seguridad.
- Jefe SSO: Reevaluación de medidas de seguridad existentes, para prevenir futuros incidentes similares.
- Personal SSO: Proporcionar capacitaciones continuas a los colaboradores de la empresa sobre como identificar y manejar situaciones de extorsión o terrorismo.
- Gerente de la sucursal: Mantener colaboración o contacto con un servicio efectivo de seguridad privada para futuras situaciones.

<b>Fecha de Actualización</b>	<b>Versión</b>	<b>Uso interno de la empresa</b>
31/01/2024	1	Confidencial

## 7 ANEXOS

### 7.1 Directorio de Continuidad

El presente directorio detalla un listado de números de contactos que permiten la gestión del riesgo relacionado, durante la contingencia:

#### 7.1.1 Contingencia 1: Caída del Sistema ERP

Nombre	Número	Descripción
Ext. Área TIC	Confidencial	Consultas y comunicados relacionadas a intermitencias o caídas del sistema informático.
Ext. Gerencia de Sucursal	Confidencial	Consultas relacionadas a la aprobación de documentación
Ext. Área de Logística	Confidencial	Consultas relacionadas al despacho de productos
Empresa Provedora del Sistema	Confidencial	Proveedor del Sistema
Consultores informáticos	Confidencial	Consultas relacionadas al sistema informático

#### 7.1.2 Contingencia 2: Rotura de Stock

Nombre	Número	Descripción
Ext. Área Comercial	Confidencial	Consultas relacionadas a la detección de rotura de stock
Ext. Área Logística	Confidencial	Consultas relacionadas a la recepción y verificación del producto.
Ext. Área Compra	Confidencial	Consultas relacionadas a la solicitud del producto.
Proveedor Nacional	Confidencial	Adquisición del producto
Proveedor Internacional	Confidencial	Adquisición del producto

#### 7.1.3 Contingencia 3: Ataques de extorsión

Nombre	Número	Descripción
Servicio Integrado de Seguridad	911	Llamadas de emergencia que integran diferentes agencias de seguridad.
UNASE	18000335486	Canal de asesoramiento de la UNASE

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial

EMPRESA DE COOMERCIALIZACIÓN DE EQUIPOS INDUSTRIALES	MANUAL DE PROCESOS PARA GESTIÓN DE CONTINGENCIAS	Página <b>35</b> de <b>35</b>
---	---	-------------------------------

SSO	Confidencial	Ext. Área de SSO para consultas y comunicados.
Policía Nacional	101	Llamadas de emergencia del área específica.
Bomberos	102	Llamadas de atención médica
Gerente General	Confidencial	Ext. Gerente General
Subgerente Corporativo	Confidencial	Ext. Subgerente Corporativo
Gerente de Sucursal	Confidencial	Ext. Gerente de Sucursal
Trabajadora Social	Confidencial	Ext. Trabajadora Social
Jefe de Marketing y Comunicación	Confidencial	Ext. Marketing y Comunicación
Coordinador de Recursos Humanos	Confidencial	Ext. Área de Recursos Humanos

## 7.2 Números telefónicos de cooperativas de taxis

Se detalla un listado de números de cooperativas de taxis que permitirán la gestión de movilización del personal durante la contingencia 3:

- **Taxi Seguro Guayaquil – Tax Móvil**
  - **Teléfono:** 0986982427
  - **Página web:** <https://taxi-seguro-guayaquil-tax-movil.negocio.site/>
  - **Servicios en GYE y áreas cercanas:**
    - Puerto Santa Ana,
    - Bellavista
    - Urb. Villa Club
    - La joya
    - Samanes
    - Sauces
    - Urdesa
    - Guayacanes
- **Taxi Fast Travel**
  - **Teléfono:** 0962768178 - 0997507793\*
- **Coop. Taxis Mall 9 de Abril**
  - **Teléfono:** 0963395157|
  - **Ubicación:** Cdla. Vernaza Norte Mz. 20 Solar 9 detrás del Mall del Sol, Guayas, Ecuador

Fecha de Actualización	Versión	Uso interno de la empresa
31/01/2024	1	Confidencial