Maestría en

Gestión de Riesgos

Trabajo de investigación previo a la obtención del título de

Magíster en Gestión de Riesgos

AUTORES:

Alexis Raúl Fuel Claudio

Bryan Steveen González Ramírez

Kleber Joselito López Brito

Diana Carolina Cardenas Esquivel

Carlos Alfonso Romero Romero

Ricardo Emmanuel Yagual Panchana

TUTORES:

Docentes titulación

David G. Benavides Gutiérrez

Paloma Manzano Martínez

Enrique Molina Suárez

Elaboración del manual de la norma ISO 31000:2018 gestión de riesgo en la empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A

Quito, junio del 2025

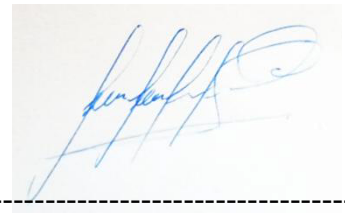
Certificación de autoría

Nosotros, **Alexis Raúl Fuel Claudio, Bryan Steveen González Ramírez, Kleber Joselito López Brito, Diana Carolina Cardenas Esquivel, Carlos Alfonso Romero Romero, Ricardo Emmanuel Yagual Panchana, declaramos** bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

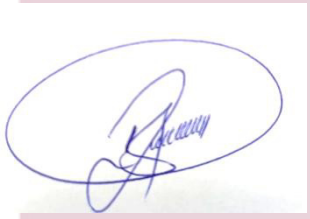
Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Alexis Raúl Fuel Claudio

Bryan Steveen González Ramírez

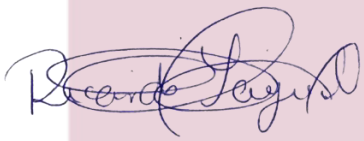


Kleber Joselito López Brito



Diana Carolina Cárdenas Esquivel

Carlos Alfonso Romero Romero



Ricardo Emmanuel Yagual Panchana

Autorización de Derechos de Propiedad Intelectual

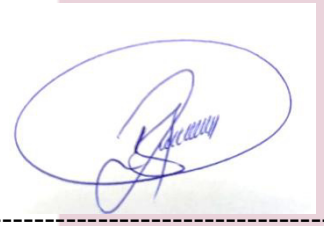
Nosotros, **Alexis Raúl Fuel Claudio, Bryan Steveen González Ramírez, Kleber Joselito López Brito, Diana Carolina Cardenas Esquivel, Carlos Alfonso Romero Romero**, **Ricardo Emmanuel Yagual Panchana**, en calidad de autores del trabajo de investigación titulado ***Titulo del trabajo de investigación Elaboración del manual de la norma ISO 31000:2018 gestión de riesgo en la empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, junio del 2025

Alexis Raúl Fuel Claudio

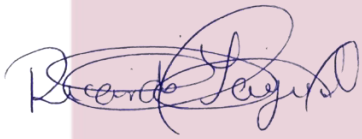
Bryan Steveen González Ramírez

Kleber Joselito López Brito



Diana Carolina Cárdenas Esquivel

Carlos Alfonso Romero Romero



Ricardo Emmanuel Yagual Panchana

Aprobación de dirección y coordinación del programa

Nosotros, **Paloma Manzano Martínez y David G. Benavides Gutiérrez,** declaramos que los graduandos: **Alexis Raúl Fuel Claudio, Bryan Steveen González Ramírez, Kleber Joselito López Brito, Diana Carolina Cardenas Esquivel, Carlos Alfonso Romero Romero, Ricardo Emmanuel Yagual Panchana** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

MANZANO MARTINEZ PALOMA - 24244436K
Firmado digitalmente por MANZANO MARTINEZ PALOMA - 24244436K
Fecha: 2025.07.28 10:39:01 +02'00'

Paloma Manzano Martínez
Director/a de la
Maestría en Gestión de Riesgos

Firmado electrónicamente por:
DAVID GENARO BENAVIDES GUTIERREZ
Validar únicamente con FirmaEC

David G. Benavides Gutiérrez
Coordinador/a de la
Maestría en Gestión de Riesgos

DEDICATORIA

Quiero expresar mi más profundo agradecimiento a todas las personas que han sido parte fundamental en este importante logro académico. A mi esposo, por su amor, paciencia y apoyo incondicional durante todo este proceso; gracias por creer en mí incluso en los momentos más difíciles. A mi hijo, mi mayor inspiración, por recordarme cada día el verdadero sentido del esfuerzo y la superación. A mis padres, por ser ejemplo de dedicación, esfuerzo y valores; su amor y confianza han sido el motor que me impulsó a seguir adelante. A mis hermanos, por su constante aliento, cercanía y compañía, que han sido esenciales en cada etapa de este camino. A mis amigos, por su comprensión, palabras de ánimo y por estar presentes en cada momento importante. Cada uno de ustedes ha dejado una huella imborrable en este proceso, brindándome fuerza cuando más lo necesitaba. Este trabajo no es solo un logro personal, sino el reflejo del apoyo, cariño y compromiso de quienes me rodean. A todos, gracias por acompañarme en esta etapa, por su fe en mí y por ser parte de este sueño cumplido.

Alexis Raúl Fuel Claudio

En primer lugar, y, sobre todo, agradezco a mi ser supremo, omnipotente, omnipresente y omnisciente que ha trazado un camino en el cual me acompaña desde el inicio de mi existencia hasta cuando él decida que debo transitar, siendo el artífice de mi destino.

A mis amados padres, Angel González Arieta y Nancy Ramírez Laime, por ser la luz en todo momento guiando mis pasos a lo largo de mi vida, convirtiéndose en el pilar fundamental en la construcción de esta historia que cada vez tiene una nueva página con escritos diferentes.

Al “Kempachi”, lo ves, ¡uno más!

Finalmente, agradezco a cada una de las personas que han sido parte de esta importante consecución.

Bryan Steveen González Ramírez

Dedico este trabajo con profundo respeto y sincera gratitud a quienes han sido los pilares esenciales en este viaje académico y personal.

A mis padres, por haber sembrado en mí los valores de la responsabilidad, la disciplina, el esfuerzo y la superación. Su ejemplo de vida, su amor incondicional y su fe constante han sido mi guía silenciosa en cada paso de este camino. Todo lo que soy y lo que he logrado, tiene sus raíces en lo que me enseñaron con palabras y, sobre todo, con hechos.

A mi esposa e hijos, por acompañarme con amor, paciencia y comprensión en los momentos más exigentes de esta etapa. Su presencia discreta pero firme, su aliento y su capacidad de sacrificio han sido una fuente de fortaleza inagotable. Este logro es también suyo, pues lo alcanzamos juntos.

Y finalmente, a quienes creen en la importancia de gestionar los riesgos con conocimiento técnico, pero también con ética, compromiso y sensibilidad social. A todos ustedes, dedico este logro con humildad y esperanza, valores que siempre me han guiado y seguirán acompañándome.

Kleber Joselito López Brito

Dedico este proyecto que ha significado un año de dedicación y esfuerzo a mis amados hijos Dannita y Mateo que han tenido que enfrentar la realidad de una madre ausente dedicada a su trabajo y estudios, a mi amado esposo Kleber López que no ha dejado que desmaye a pesar de las adversidades y especialmente con profundo amor y gratitud a mis padres Luz y Holguer que cada día me enseñan que el rol de padres no acaba jamás; han sido el pilar fundamental en mi vida. A todos los nombrados, gracias por su apoyo incondicional, por creer en mí y enseñarme el valor del esfuerzo y la perseverancia. Son mi fuente de constante de motivación, por su comprensión en los momentos difíciles y por celebrar conmigo cada logro alcanzado, aunque sea grande o pequeño.

A Dios, por darme la fortaleza, sabiduría y salud para seguir adelante en este camino, por no abandonarme nunca y enseñarme que sus tiempos son perfectos.

Y a todas las personas que, de alguna manera, me acompañaron en este proceso. Cada palabra de aliento, cada gesto de apoyo y cada enseñanza han sido parte esencial en la construcción de este logro.

Diana Carolina Cardenas Esquivel

Este proyecto lo dedico con todo cariño a mis queridos padres que día a día me han inculcado a seguir mejorando, a través de valores sólidos, a no quedarme estancado y siempre a mirar lo positivo de la vida, a mirar en cada una oportunidad una meta de logro y satisfacción basada en el esfuerzo y sacrificio constante. Que a pesar de cualquier adversidad lo importante es continuar, que la actitud dice mucho de las personas y que si queremos triunfar en la vida debemos sonreír y poner todo de nuestro ser para lograrlo. A mis queridos hijos y esposa ya que sin el cariño y comprensión de ellos no habría sido posible culminar este proceso, difícil sí, pero con el regocijo de llegar a una meta, de enseñarles a mis hijos el valor de estudiar y prepararse para la vida, de ser profesionales y sobre todo ser buenos seres humanos, de dar cada día un valor agregado a las cosas que hacemos y sobre todo la constancia para alcanzar las metas planteadas.

Carlos Alfonso Romero Romero

Dedico este logro en primer lugar a Dios, por mantenerme con salud y bienestar durante este nuevo reto académico para la obtención de mi título de cuarto nivel.

A mi mamá, Yleana Del Rocío Yagual Panchana, quien ha sido y siempre será mi mayor ejemplo a seguir, la que me motiva y ayuda día a día para no rendirme y seguir adelante con nuevos objetivos universitarios, todos los esfuerzos que has realizado por mí los verás reflejados en un profesional de calidad, honesto y responsable con mis obligaciones.

A mi abuelita, Violeta Natividad Yagual Panchana, por ser ejemplo de fuerza y carácter, quien me ha educado con valores y con ejemplo de que hay que esforzarse todos los días para que los resultados lleguen, agradeciéndole todos los consejos y cariño que me ha brindado desde el día uno.

A mi querida familia y amigos, que han estado pendientes de mí en todo mi proceso académico, brindándome fuerzas, cariño y motivos para seguir enfocado en la meta y poder escalar un peldaño más en la vida.

Ricardo Emmanuel Yagual Panchana

AGRADECIMIENTOS

Agradecemos profundamente a la Universidad Internacional del Ecuador por habernos brindado la invaluable oportunidad de formarnos en un entorno académico caracterizado por la excelencia, el compromiso y una visión profundamente humanista. Esta institución ha sido un pilar esencial en nuestro crecimiento profesional y personal, proporcionándonos las herramientas necesarias para enfrentar los desafíos de la gestión de riesgos con responsabilidad, ética y rigor técnico.

Expresamos nuestra especial gratitud a la Magíster Paloma Manzano Martínez, directora de la Maestría en Gestión de Riesgos, por su liderazgo inspirador, su dedicación incansable y su acompañamiento constante a lo largo de este proceso. Su guía ha sido un faro de motivación y confianza, que supo encauzar cada esfuerzo hacia la excelencia académica.

Finalmente, a todas las personas que, de una u otra manera, formaron parte de esta travesía, les extendemos nuestro más sincero y profundo agradecimiento. Cada gesto, palabra o acción ha dejado una huella en este logro que hoy celebramos con humildad y gratitud.

RESUMEN

El presente estudio analizó los desafíos y avances en la protección de datos personales dentro del entorno empresarial, especialmente en el contexto ecuatoriano tras la entrada en vigor de la Ley Orgánica de Protección de Datos Personales, identificando como principales riesgos las amenazas de acceso no autorizado, riesgos de ciberdelincuencia, el manejo inadecuado de información y la falta de conocimiento legal sobre la normativa vigente, asimismo, se examinaron las limitaciones legales, técnicas y éticas que condicionaron la investigación y el tratamiento de datos personales, destacando la importancia del consentimiento informado, la finalidad del tratamiento y la minimización de datos como principios fundamentales para garantizar la privacidad y los derechos de los titulares, concluyendo que la protección de datos personales es un derecho fundamental derivado del derecho a la vida privada y la intimidad, que adquirió mayor relevancia en la era digital debido a la facilidad de almacenamiento y distribución de información sensible, y aportando a la investigación propuestas de buenas prácticas, protocolos de seguridad y recomendaciones para fortalecer la cultura organizacional orientada a la privacidad, así como la necesidad de una mayor sensibilización y formación continua en materia de protección de datos tanto para la organización como para los proveedores, clientes y colaboradores.

Palabras Clave: ciberseguridad, confidencialidad, información, riesgo, seguridad

ABSTRACT

This study analyzed the challenges and advances in the protection of personal data within the business environment, especially in the Ecuadorian context after the entry into force of the Organic Law on Personal Data Protection, identifying as main risks the threats of unauthorized access, risks of cybercrime, inadequate handling of information and lack of legal knowledge about current regulations, likewise, the legal, technical and ethical limitations that conditioned the investigation and processing of personal data were examined, highlighting the importance of informed consent, the purpose of the treatment and data minimization as fundamental principles to guarantee the privacy and rights of the owners, concluding that the protection of personal data is a fundamental right derived from the right to private life and intimacy, which acquired greater relevance in the digital age due to the ease of storage and distribution of sensitive information, and contributing to the research with proposals for good practices, security protocols and recommendations to strengthen the organizational culture oriented towards privacy, as well as the need for greater awareness and continuous training in data protection for both the organization and its suppliers, clients and collaborators.

Keywords: cybersecurity, confidentiality, information, risk, security

TABLA DE CONTENIDOS

ACUERDO DE CONFIDENCIALIDAD **4**

CAPITULO 1 ..... **21**

INTRODUCCIÓN 21

1. PLANTEAMIENTO DEL PROBLEMA E IMPORTANCIA DEL ESTUDIO *22*

1.1. Definición del proyecto 22

1.2. Naturaleza o tipo de proyecto 24

1.3. Objetivos 25

1.3.1. Objetivo general 25

1.3.2. Objetivo especifico 25

1.4. Justificación e importancia del trabajo de investigación 26

CAPITULO 2 ..... **28**

LA ORGANIZACIÓN 28

2. PERFIL DE LA ORGANIZACIÓN *28*

2.1. Nombre, actividades, mercados servidores y principales 28

2.1.1. Nombre de la empresa 28

2.1.1. Misión, visión, valores 28

2.1.3. Actividades, marcas, productos y servicios 30

2.1.4. Ubicación de la sede 30

2.1.5. Ubicación de las operaciones 30

2.1.6. Propiedad y forma jurídica 31

2.1.7. Mercados servidos o ubicación de sus actividades 32

2.1.8. Tamaño de la organización 32

2.1.9. Información sobre empleados y otros trabajadores 32

2.1.10. Procesos claves relacionados con el objetivo propuesto 34

2.1.11. Principales cifras, ratios y números que definen a la empresa 34

2.1.12. Modelo de Negocio 34

2.1.13. Grupo de interés internos y externos 34

2.1.14. Otros datos de interés 36

CAPITULO 3 ..... **37**

DOCUMENTOS DE SEGURIDAD 37

3. DESARROLLO DEL CONTENIDO *37*

3.1. Análisis de Riesgos 37

3.1.1. Identificación de la organización y de sus centros de trabajo 37

3.1.2. Representante legal y Responsable de seguridad 37

3.1.3. Actividades de la organización 37

3.1.4. Tratamientos de la organización y sus riesgos 38

3.1.5. Consentimientos y notas afirmativas 39

3.2. Registro de actividades de Tratamiento 42

3.2.1. Grupos de información 42

3.2.2. Sistemas de tratamiento y niveles de seguridad 43

3.2.3. Finalidades, categorías de datos, de interesados y de destinatarios 45
3.2.4. Encargados de tratamientos 45
3.3. Registro de Dispositivos (Dispositivos digitales) 46
3.4. Registros de Sistemas de información (Software, seguridad, etc.) 47
3.5. Registro de personal 48
3.5.1. Con acceso a Datos 48
3.5.2. Sin acceso a Datos 49
3.5.3. Accesos Físicos 49
3.6. Registro de prestadores de servicio 50
3.6.1. Con acceso a datos catalogados 50
3.6.2. Sin acceso a datos catalogados 51
3.7. Sistemas de captación de imágenes y audio 52
3.7.1. Número de cámaras 53
3.7.2. Zonas de influencia 54
3.7.3. Sistema de tratamiento y almacenamiento 54
3.7.4. Usuarios autorizados 54
3.8. Dispositivos Medidas de seguridad 54
3.8.1. Análisis de las medidas de seguridad de los dispositivos 54
3.8.2. Propuesta de mejora de las medidas de seguridad 58
3.9. Puestos de trabajo 59
3.9.1. Análisis de las medidas de seguridad de cada puesto de trabajo, según la información tratada 59
3.9.2. Acuerdo de confidencialidad 61
3.10. Encargado del tratamiento 65
3.10. Contrato E. Tratamiento 66
3.11. Análisis web 70
3.11.1. Análisis, configuración y política de cookies 71
3.11.2. Formularios de contacto, newsletter, trabaja conmigo, registro 73
3.11.3. Avisos Legales 79
3.12. Medidas de seguridad 80
3.12.1. Análisis, uso y medidas de seguridad en el uso de navegadores 80
3.12.2. Hosting y Servidores 84
3.12.2.1. Medidas de seguridad 87
3.12.2.2. Prestadores de servicios 89
3.12.3. Gestores de Correo electrónico 90
3.12.3.1. Medidas de seguridad 90
3.12.3.2. Prestadores de servicios 92

CAPITULO 4 95

CONFECCIÓN DE UN PLAN DIRECTOR DE SEGURIDAD 95
4. DESCRIPCIÓN DE LO QUE ES UN PLAN DIRECTOR DE SEGURIDAD Y LOS BENEFICIOS PARA LA EMPRESA 95
4. 1. Check List PDS 96
4.1.1. Análisis de la situación actual de la empresa 102
4.1.2. Plan estratégico en materia tecnológica 108
4.2. Verificación de Controles 112
4.3. Inventario de Activos 117
4.4. Análisis de Riesgos 120
4.5. Clasificación y Priorización. 130
4.6. Check List PDS. 132

CAPITULO 5 ..... **135**

PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO 31000:2028 135

5. DESARROLLO DEL CONTENIDO *135*

5.1. Objeto y campo de aplicación 135

5.2. Referencias Normativas 137

5.3. Términos y definiciones 138

5.4. Principios de Gestión del Riesgo 139

5.4.1. Integrada 140

5.4.2. Estructuradas y exhaustiva 140

5.4.3. Adaptada 140

5.4.4. Inclusiva 141

5.4.5. Dinámica 141

5.4.6. Mejor información disponible 141

5.4.7. Factores humanos y culturales 142

5.4.8. Mejora continua 142

5.5. Marco de referencia 142

5.5.1. Generalidades 142

5.5.2. Liderazgo y compromiso 143

5.5.3. Integración 144

Fuente: Organigrama Estructural Detallado Fuente: Multitableros & Herrajes, S.A. (2025) 146

5.5.4. Diseño 147

5.5.4.1. Comprensión de la organización y su contacto 148

5.5.4.2. Articulación del compromiso con la gestión del riesgo 151

5.5.4.3. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización 155

5.5.4.4. Asignación de recursos 157

5.5.4.5. Establecimiento de la comunicación y la consulta 160

5.5.5. Implementación 161

5.5.6. Valoración 162

5.5.7. Mejora 163

5.5.7.1. Adaptación 163

5.5.7.2. Mejora continua 163

5.6. Proceso 165

5.6.1. Generalidades 165

5.6.2. Comunicación y consulta 166

5.6.3. Alcance, contexto y criterios 167

5.6.3.1. Generalidades 167

5.6.3.2. Definición del alcance 167

5.6.3.3. Contextos externo e interno 172

5.6.3.4. Definición de los criterios de riesgo 173

5.6.4. Evaluación del riesgo 175

5.6.4.1. Generalidades 175

5.6.4.2. Identificación del riesgo 176

5.6.4.3. Análisis del riesgo 177

5.6.4.4. Valoración del riesgo 178

5.6.5. Tratamiento del riesgo 179

5.6.5.1. Generalidades 179

5.6.5.2. Selección de las opciones para el tratamiento del riesgo 179

5.6.5.3. Preparación e implantación de los planes de tratamiento del riesgo 179
5.6.6. Seguimiento y revisión 180
5.6.7. Registro e informe 181
5.6.7.1. Medios de comunicación 181
5.6.7.2. Cronograma de actividades para la implementación de procesos de mejora ante los riesgos detectados 181
5.6.8. Auditoría interna 182
5.6.8.1. Objetivos de la Auditoría interna 182
5.6.8.2. Procesos de la Auditoría interna 182
5.6.8.3. No conformidades y acciones correctivas 186

CAPITULO 6 188

6. CONCLUSIONES Y APLICACIONES 188
6.1. Conclusiones generales 188
6.2. Conclusiones específicas 189
6.2.1. Análisis del cumplimiento de los objetivos de la investigación 189
6.2.2. Contribución a la gestión empresarial 190
6.2.3. Contribución a nivel académico 191
6.2.4. Contribución a nivel personal 191
6.3. Limitaciones a la Investigación 192

BIBLIOGRAFÍA 194

ANEXOS 196

LISTA DE TABLAS

Tabla 1 37
Tabla 2 44
Tabla 3 45
Tabla 4 46
Tabla 5 46
Tabla 6 47
Tabla 7 48
Tabla 8 49
Tabla 9 49
Tabla 10 51
Tabla 11 59
Tabla 12 90
Tabla 13 91
Tabla 14 96
Tabla 15 98
Tabla 16 99
Tabla 17 101
Tabla 18 109
Tabla 19 110
Tabla 20 112
Tabla 21 117
Tabla 22 120
Tabla 23 130
Tabla 24 132
Tabla 25 136
Tabla 26 149
Tabla 27 158
Tabla 28 160
Tabla 29 175
Tabla 30 176
Tabla 31 176
Tabla 32 177
Tabla 33 177
Tabla 34 177
Tabla 35 178
Tabla 36 180
Tabla 37 181

Tabla 38 181
Tabla 39 186

LISTA DE FIGURAS

Figura 1.....30
Figura 2.....30
Figura 3.....31
Figura 4.....32
Figura 5.....55
Figura 6.....56
Figura 7.....57
Figura 8.....74
Figura 9.....75
Figura 10.....76
Figura 11.....77
Figura 12.....145
Figura 13.....156
Figura 14.....165
Figura 15.....174

CAPITULO 1

INTRODUCCIÓN

En la época digital que estamos viviendo, la seguridad de la información se ha convertido en lo más importante de la organización y de las empresas que compiten en el mercado, la correcta gestión, manipulación y protección de datos garantiza la continuidad de la empresa y salvaguarda la confianza de los clientes y los trabajadores. En el país, varias empresas pequeñas y medianas todavía no han incorporado una base sólida de seguridad y gestión de riesgos en sus negocios, lo que las expone a diferentes riesgos operacionales de alto impacto.

La Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., ubicada en la ciudad de Quevedo, logró consolidarse como una de las ferreterías más concurridas de la zona, gracias a la experiencia ferretera de muchos años en el mercado brindando productos de calidad a sus clientes, sin embargo, como muchas empresas en crecimiento y en etapa de modernización en el país, carece de un sistema estructurado en la gestión de riesgos. Esta situación compromete y hace vulnerable a la reputación corporativa.

En un análisis preliminar realizado en la empresa, se pudo detectar que, si bien existen prácticas básicas sobre la protección de datos sensibles y procedimientos internos, prácticamente no se cuenta con una normativa estandarizada que pueda garantizar la seguridad de datos ante posibles riesgos. Los protocolos ante incidentes y la escasez de una organización evidencian la necesidad de implementar estrategias en el área en cuestión.

En el presente trabajo se propone desarrollar un manual de gestión de riesgos basado en la norma ISO 31000:2018. Esta norma es un estándar internacionalmente reconocido que proporciona las directrices y los principios para una gestión rápida y sólida de los riesgos, es aplicable a cualquier tipo de organización y se desarrollará eficazmente en la ferretería.

La implementación de la norma ofrece varios beneficios en la empresa como el mejoramiento de la capacidad de reacción y acciones para anticiparse a las diferentes amenazas que puedan ocurrir, fortaleciendo el cumplimiento normativo y optimizando los procesos y recursos. Al adoptar esta norma, la empresa podrá integrar la gestión de riesgos, promoviendo las decisiones y los procesos de forma integrada mejorando el desempeño de la empresa.

1. PLANTEAMIENTO DEL PROBLEMA E IMPORTANCIA DEL ESTUDIO

1.1. Definición del proyecto

Seguridad de la información es el conjunto de medidas, políticas, procedimientos y controles destinados a proteger la información confidencial de la organización frente a accesos no autorizados, usos indebidos, interrupciones o destrucciones, abarcando tanto aspectos digitales como físicos y de entorno. En el contexto de la Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A Multitableros & Herrajes S.A., tiene un proyecto de seguridad de la información que implica la elaboración de un manual de la norma ISO 31000:2018 gestión de riesgo en la empresa que garantice la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos de la empresa (GLOBAL SUITE SOLUTIONS, 2023).

En la actualidad, los riesgos son inherentes respecto a las organizaciones, es decir, son inevitables y difícilmente pueden ser eludidos, pero mediante la aplicación de estrategias, herramientas y estándares se los podría reducir significativamente (Syafaqah & Ristati, 2022).

Bajo esta óptica, las organizaciones se enfrentan a una diversidad de riesgos y amenazas potenciales, que van desde riesgos tradicionales hasta emergentes como fue el caso del COVID-19, exponiendo las vulnerabilidades y debilidades de las empresas sin importar si son grandes o pequeñas. Las consecuencias e impactos radican en la falta o ausencia de sistemas de resiliencia o adaptabilidad con relación a los riesgos, creando una crisis en las organizaciones e inclusive produciendo la desaparición o cierre de muchas empresas.

Es importante recalcar o mencionar problemas comunes a los que están expuestos las empresas hoy en día:

- Incidentes cibernéticos.
- Interrupción del negocio.
- Crisis energética.
- Cambios en la legislación y regulación.
- Catástrofes naturales.
- Cambio climático.

- Escasez de mano de obra calificada.
- Riesgos políticos y violencia.
- Evolución del mercado.
- Brote pandémico.
- Nuevas tecnologías.
- Robo, fraude y corrupción.

Bajo este contexto y con los factores mencionados con anterioridad, la inexistencia de un sistema o plan de gestión de riesgos cuya finalidad sea mitigar o reducir los riesgos, y sumado la falta de conocimiento en temas enfocados a la gestión de riesgos; nace la necesidad de la implementación de la norma ISO 31000:2018 en la empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes", cuyo objetivo será la resiliencia y adaptabilidad a los riesgos y sus impactos.

1.2. Naturaleza o tipo de proyecto

El presente trabajo que estamos realizando es un proyecto de diseño, porque parte de la estructuración de un sistema funcional y práctico, basado en fundamentos teóricos que permiten realizar acciones con soluciones adaptadas a las necesidades específicas de la empresa ferretera, para buscar el mejor desempeño en los diferentes procesos y funciones.

Este proyecto integra los lineamientos de la norma ISO 31000:2018, que se basa en la gestión de riesgos, por lo tanto, el proyecto no solo busca mejorar la productividad y la eficiencia de la organización, sino también, identificar y minimizar o corregir permanentemente los riesgos a los que se expone, aplicando esta norma garantizaremos un sistema adaptable y resiliente que pueda anticiparse a problemáticas que perjudiquen significativamente al progreso de la empresa.

A través de un análisis profundo, el proyecto planteó soluciones novedosas que impulsaron mejoras significativas en los procedimientos internos, promoviendo un lugar de trabajo más seguro, eficiente y comprometido su entorno.

1.3. Objetivos

1.3.1. Objetivo general

- Diseñar e implementar un manual de gestión de riesgos basado en la norma ISO 31000:2018, que sea aplicable a la Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A., con la finalidad de fortalecer, resguardar y mejorar la seguridad de la empresa

1.3.2. Objetivo especifico

- Identificar, analizar y evaluar los riesgos en todas las actividades y funciones significativas de la empresa, considerando tanto amenazas como oportunidades relevantes para la organización.

- Prevenir, detectar y responder a amenazas y vulnerabilidades informáticas con procedimientos claros para los riesgos de la información de la empresa (datos, sistemas, infraestructura).

- Garantizar la confidencialidad, integridad y disponibilidad de la información con el cumplimiento de normativas y estándares legales que rigen en el Ecuador.

- Evaluar los riesgos actuales en la empresa "Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes", con la finalidad de generar un plan de gestión de riesgos cuya finalidad sea reducir o mitigar los impactos que puedan ocasionar a la organización.

1.4. Justificación e importancia del trabajo de investigación

La gestión de riesgos en la actualidad es de suma importancia para el mundo empresarial debido a su complejidad y dinamismo debiendo comprender que nos encontramos al momento frente a una diversa gama de riesgos, que pueden afectar a su sostenibilidad en el mercado, así como el éxito que podrían tener. Por ello es importante mantener procesos de identificación para poder evaluar y mitigar los riesgos que una organización enfrenta en las actividades cotidianas, así como en un ámbito más complejo.

Según (Rodríguez Quimí, 2023) "La aplicación eficaz de esta normativa no solamente beneficiaría a la empresa, sino también a la sociedad, generando un impacto positivo en esta, siendo la empresa un referente importante para sus comunidades aledañas, contribuyendo y apoyando al desarrollo

económico.”. La empresa ferretera contribuye a sus clientes con productos de calidad, ayudando y potenciando al desarrollo de su entorno.

La gestión de riesgos es un proceso clave en los proyectos, debido a que se identifican, analizan, valoran y monitorean los riesgos, para reducir la incertidumbre en toda la organización, trayendo beneficios como la mejora en la toma de decisiones y reducción de pérdidas económicas y humanas. Todos los proyectos pueden sufrir riesgos constantemente, por lo cual, es muy importante implementar la gestión de riesgos en nuestra organización, caso contrario, las amenazas pueden materializarse y afectar gravemente a la empresa, entre las más comunes tenemos los accidentes de los trabajadores, retrasos en productos y la suspensión de las actividades de la empresa. (Molina Moreno, Espitia Mojica, & Suárez Vargas, 2022).

CAPITULO 2

LA ORGANIZACIÓN

2. PERFIL DE LA ORGANIZACIÓN

La Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A., cuenta con 14 Años de Experiencia, consolidada como un referente confiable en el suministro de productos de alta calidad y una amplia gama de productos de ferretería, materiales y mantenimiento del hogar.

Posee clientes que incluyen tanto a profesionales del sector de la construcción como a consumidores particulares interesados en mejorar sus hogares, ofreciendo un servicio excepcional, asesoramiento experto y una amplia gama de productos que satisfacen las necesidades de los clientes (Multitableros & Herrajes S.A., 2025).

2.1. Nombre, actividades, mercados servidores y principales

2.1.1. Nombre de la empresa

Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.

2.1.1. Misión, visión, valores

Misión

La empresa Multitableros & Herrajes S.A. tiene como misión proporcionar a sus clientes productos ferreteros con altos estándares de calidad, con un servicio eficiente y precios módicos. La empresa

busca satisfacer las necesidades de sus consumidores mediante una atención personalizada y especializada, con una oferta que combine disponibilidad, variedad y responsabilidad comercial.

Visión

La empresa Multitableros & Herrajes S.A. busca consolidarse como una de las principales ferreterías a nivel país, destacando por su capacidad de ofrecer productos de alta calidad y un servicio técnico especializado. Su visión a mediano plazo es ser reconocida por su responsabilidad con los clientes, la atención personalizada y la mejora continua, aportando al crecimiento del sector ferretero.

Valores

Responsabilidad: Cumplir con los compromisos de trabajo con clientes, colaboradores y proveedores, de manera ética y oportuna.

Compromiso con el cliente: Brindar una atención de calidad, eficaz y honesta, enfocada en resolver las necesidades reales de cada proyecto.

Seguridad: Priorizar la seguridad de los trabajadores y clientes, promoviendo prácticas que prevengan riesgos e incentivando a la seguridad empresarial.

2.1.3. Actividades, marcas, productos y servicios

La Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A., ofrece una amplia gama de productos de ferretería y materiales para el hogar, incluyendo categorías como: Herrajes, Materiales para baños, Materiales de construcción, Materiales eléctricos, Madera procesada, Materiales de plomería, Pinturas, Ferretería general, Decoraciones y Pegamentos.

Figura 1

Imagen de la empresa

Fuente: *Página Web de la empresa multitableros.store*

2.1.4. Ubicación de la sede

Sede principal en Quevedo, provincia de Los Ríos, Ecuador.

2.1.5. Ubicación de las operaciones

Av. Principal Vía a Babahoyo, Quevedo, Los Ríos, Ecuador.

Figura 2

Ubicación de la Empresa

Fuente: *Página Web de la empresa multitableros.store*

Figura 3

Fachada de la empresa

Fuente: *Red Social Facebook de la empresa*

2.1.6. Propiedad y forma jurídica

La empresa es de propiedad privada, constituida como una sociedad anónima (S.A.), lo que implica que su capital está dividido en acciones y pertenece a los accionistas que la conforman.

2.1.7. Mercados servidos o ubicación de sus actividades

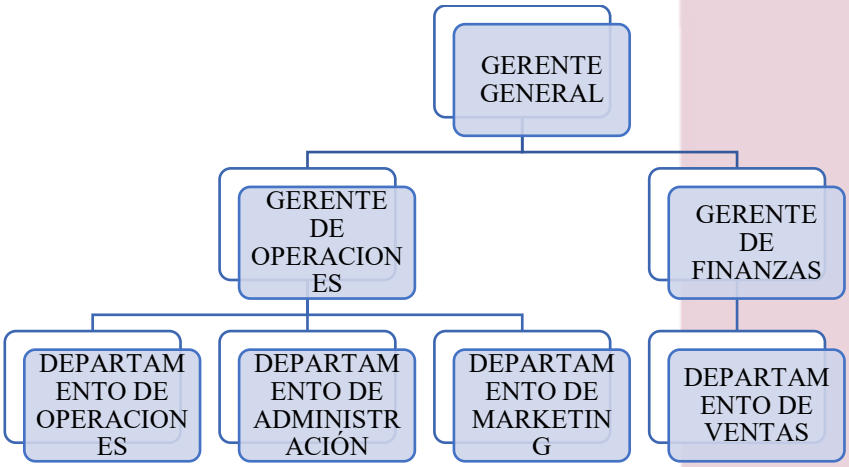
Mercado Local: Principalmente atiende a clientes en el cantón Quevedo y la provincia de Los Ríos, ofreciendo productos y servicios a particulares, constructoras, carpinteros y empresas vinculadas a la construcción y remodelación.

2.1.8. Tamaño de la organización

Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. es una empresa de tamaño pequeño según estándares internacionales y nacionales de clasificación empresarial.

Figura 4

Organigrama de la empresa



Fuente: *Orgánico funcional documentación de la empresa*

2.1.9. Información sobre empleados y otros trabajadores

Actualmente, emplea a 21 personas, dentro de las cuales como política de la empresa se busca llegar a una equidad de género, es por ello que actualmente se cuenta con trece hombres y ocho mujeres,

desempeñándose en sus cargos y funciones a través de contratos indefinidos. Se encuentran con edades desde los 19 años hasta 42 años, con un promedio de aproximadamente de 30 años.

Estructura Organizativa

Gerencia

- Gerente General
- Gerente de Operaciones
- Gerente de Finanzas

Departamento de Ventas (6 empleados)

1. Jefe de Ventas

2. Vendedores (5)

Departamento de Marketing (1 empleados)

1. Jefe de Marketing

Departamento de Operaciones (5 empleados)

1. Jefe de Operaciones

2. Especialistas en Operaciones (3)

4. Encargado de Logística

Departamento de Administración (3 empleados)

2. Especialista en Recursos Humanos

3. Contador

5. Recepcionista

2.1.10. Procesos claves relacionados con el objetivo propuesto

Mercado Local: Principalmente atiende a clientes en el cantón Quevedo y la provincia de Los Ríos.

Enfoque de Servicio: La empresa se especializa en la venta al por menor y mayor de materiales de construcción, adaptándose tanto a proyectos domésticos como industriales.

Comercio Exterior: Importa insumos de países como España, China, Hong Kong, Colombia y Turquía, aunque sus ventas se concentran en el mercado nacional.

2.1.11. Principales cifras, ratios y números que definen a la empresa

Desempeño Financiero, en 2023, la empresa registró una caída de ingresos netos del 1,48%, pero su activo total creció en un 107,16% y el margen neto aumentó en un 0,15% (EMIS, 2025).

2.1.12. Modelo de Negocio

Elementos clave del modelo de negocio son la propuesta de valor, productos de calidad, servicio diferenciado y precios competitivos.

2.1.13. Grupo de interés internos y externos

Los segmentos de clientes son pequeños constructores y contratistas, carpinteros y talleres de fabricación de muebles y estructuras, por último, personas particulares y propietarios de viviendas.

Entre los grupos de interés se tiene personas o grupos que buscan un beneficio directo o indirecto en la empresa, entre los cuales tenemos:

Grupos de interés interno:

- Empleados
- Propietarios o accionistas
- Gerentes y directivos

Grupos de interés externos:

- Clientes
- Proveedores
- Competidores
- Reguladores o autoridades
- Comunidad local
- Bancos e instituciones financieras
- Asociaciones y gremios

Es importante identificar los grupos de interés ya que mejora significativamente la toma de decisiones, considerando las necesidades y expectativas, fomentando la comunicación efectiva, y sobre todo respondiendo a sus necesidades, además de que la empresa puede gestionar los riesgos y oportunidades de manera más efectiva.

2.1.14. Otros datos de interés

Otros datos de interés: cuenta con canales de distribución como son la venta directa en tienda principal, servicios complementarios como la entrega a domicilio y servicios de corte personalizado de tableros de madera, melamina o MDF, y canales digitales a través de redes sociales y sitio web.

CAPITULO 3

DOCUMENTOS DE SEGURIDAD

3. DESARROLLO DEL CONTENIDO

3.1. Análisis de Riesgos

3.1.1. Identificación de la organización y de sus centros de trabajo

Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. tiene una sede principal en la parroquia San Cristóbal de la ciudad de Quevedo, provincia de Los Ríos, ofreciendo productos y servicios a particulares, constructoras, carpinteros y empresas vinculadas a la construcción y remodelación.

3.1.2. Representante legal y Responsable de seguridad

Tabla 1

Datos del representante legal de Multitableros

Representante legal	**Cargo**	**Ruc.**
LOPEZ BRITO BYRON DANIEL	Gerente	1291767172001
Representante de seguridad		
N/A	N/A	N/A

Fuente: *Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025.*

3.1.3. Actividades de la organización

La **Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A.**, la actividad económica principal es la venta al por mayor de artículos de ferreterías y cerraduras lo que incluye:

martillos, sierras, destornilladores, y otras herramientas de mano, accesorios y dispositivos; cajas fuertes, extintores como también la venta al por mayor de madera no trabajada (en bruto), de la misma manera se desarrolla la venta al por mayor de materiales de construcción: piedra, arena, grava, cemento, etcétera.

3.1.4. Tratamientos de la organización y sus riesgos

Los tratamientos que la Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A., puede implementar para gestionar sus principales riesgos, considerando su actividad en el sector ferretero y comercio minorista de materiales de construcción.

Principales Riesgos de la Organización

Riesgos Operativos

- Desabastecimiento o rotura de stock: Falta de materiales clave puede afectar la satisfacción del cliente y ventas.
- Daño o pérdida de mercadería: Robo, deterioro o manipulación inadecuada durante almacenamiento o transporte.

Riesgos Legales y de Cumplimiento

- Incumplimiento normativo: Falta de alineación con regulaciones locales e internacionales (ej. importaciones, seguridad laboral).
- Litigios o reclamos de clientes: Por productos defectuosos o servicios insatisfactorios.

Riesgos de Seguridad y Salud Ocupacional

- Accidentes laborales: Durante manipulación de materiales, cortes, carga y descarga.
- Exposición a sustancias químicas: Por el manejo de adhesivos, pinturas y otros productos.

Riesgos Tecnológicos y de Seguridad de la Información

- Ciberataques o pérdida de datos: Vulnerabilidad de sistemas informáticos y bases de datos de clientes.
- Fallas en sistemas de gestión: Interrupciones en facturación, inventario o comunicación.

Riesgos de Reputación

- Insatisfacción del cliente: Productos de baja calidad o servicio ineficiente.
- Incidentes en redes sociales o medios: Comentarios negativos o mala publicidad.

3.1.5. Consentimientos y notas afirmativas

La Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., con la finalidad de dar cumplimiento a la Ley Orgánica de Protección de Datos Personales de Ecuador (Ley Orgánica de Protección de Datos Personales, 2021), la empresa mantiene un formato de llenado libre y voluntario del consentimiento y los datos personales de los clientes y proveedores, ver **ANEXO 1.**

CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES

Quevedo, a los …….…… del mes de …….. del 2025.

En cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador, le informamos que sus datos personales serán tratados por la Empresa Ferretería Tableros Herrajes & Afines,

Multitableros & Herrajes S.A. con la finalidad de gestionar y mantener la relación comercial entre usted y nuestra empresa.

Los datos personales que se podrán tratar son los siguientes:

- Datos identificativos (como nombres y apellidos completos, número de identificación)

- Datos de contacto (como dirección física, dirección de correo electrónico, teléfono, contacto de emergencia)

-Datos económicos (información sobre cuentas bancarias, situación financiera)

-Información reflejada en documentos personales como:

Cédula
Papeleta de votación
Cualquier otro dato personal proporcionado directamente por el personal/proveedor a través de formularios o contratos suscritos entre las partes, en el marco de su relación comercial y contractual.

El tratamiento de sus datos personales se llevará a cabo de manera confidencial y se adoptarán las medidas de seguridad necesarias para proteger su privacidad.

1. La legitimidad del tratamiento de sus datos personales es el consentimiento que usted nos da al aceptar este documento. La negativa a proporcionar su consentimiento para el tratamiento de sus datos personales implica que no se podrá establecer o mantener la relación comercial.
2. Sus datos personales no serán compartidos con terceros, salvo en los casos en que sea necesario para cumplir con las obligaciones legales, órdenes judiciales, o en aquellos casos en que se requiera para el desarrollo de la relación comercial.

3. Usted tiene derecho a acceder, rectificar, suprimir, limitar u oponerse al tratamiento de sus datos personales, así como a solicitar la portabilidad de estos. Para ejercer estos derechos, puede ponerse en contacto con nosotros a través de información@ferreteríatablerosherrajes&afines.com.
4. Sus datos personales serán mantenidos en nuestros registros de forma indefinida, pero usted podrá solicitar su eliminación en cualquier momento.
5. Los datos personales otorgados a esta empresa no serán transferidos a terceros países, salvo que sea estrictamente necesario para el cumplimiento de obligaciones legales o contractuales debido a los distintos negocios e importación que se realizan, y siempre que el país receptor cuente con niveles adecuados de protección de datos personales conforme a lo establecido por la Ley Orgánica de Protección de Datos Personales en el Ecuador.

Al firmar este documento, el proveedor y/o cliente declara haber sido informado de forma clara y precisa sobre el tratamiento de sus datos personales y da su consentimiento para el tratamiento de los mismos con las finalidades indicadas anteriormente.

( ) Sí otorgo mi consentimiento ( ) No otorgo mi consentimiento	A **Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A.,** para el tratamiento de mis datos personales para las finalidades previstas en este documento.

Nombres y apellidos:	
Documento de identidad:	
Correo electrónico:	

Firma:	

3.2. Registro de actividades de Tratamiento

3.2.1. Grupos de información

La empresa **Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A.** todo el tiempo debido al movimiento de la empresa, realiza el tratamiento de datos personales de diversos grupos, según su vínculo con la misma. Por lo tanto, a continuación, se detallan los grupos de información, los tipos de datos que se recogen, y la finalidad de su tratamiento:

Clientes: Personas naturales o jurídicas que adquieren un servicio o la compra de un producto, con la finalidad de gestionar las ventas, solicitudes, enviar promociones de los productos y finalmente la facturación, en donde los datos que se tratan son: Nombres, apellidos, cédula, RUC, dirección, teléfono, correo electrónico, historial de compras, datos bancarios, que se usarán en gestión de ventas, facturación, atención al cliente.

Empleados: Está compuesta por personal operativo, vendedores, cajeros, administrativos, con la finalidad de dar seguimiento a las relaciones que mantienen con el cliente, el desempeño, controlar la asistencia y acceso diferentes áreas, como también administrar beneficios y obligaciones legales. Los datos para tratar en esta ocasión serán: Datos personales, laborales, familiares, bancarios y

evaluaciones de desempeño se usarán únicamente en el ámbito laboral para pagos de nómina y cumplimiento de obligaciones laborales.

Proveedores: Empresas que abastece de marial a la ferretería con la finalidad de gestionar relaciones comerciales como también se evalúa el desempeño y el cumplimiento en donde los datos serán: de contacto, RUC, cuentas bancarias, contratos, referencias comerciales, que serán usados en Gestión de compras, pagos, control de abastecimiento.

Prospecto a empleados: Personas que envían sus datos con el propósito de trabajar en la empresa, con la finalidad de evaluar el perfil del candidato, y contratar, en donde los que se receptan serán: Hojas de vida, datos de contacto, historial académico y laboral, referencias para ser usados en el proceso de selección.

Usuarios de canales digitales: Personal que interactúa mediante a redes sociales**,** con la finalidad de atender solicitudes, monitorear y mejorar la experiencia del usuario, es importante el manejo de los siguientes datos: IP, cookies, ubicación, comportamiento en el sitio web, datos de contacto la finalidad del tratamiento será mejorar de experiencia digital, marketing, atención a solicitudes en línea.

3.2.2. Sistemas de tratamiento y niveles de seguridad

A continuación, se describen los sistemas de tratamiento y los niveles de seguridad recomendados para cada grupo de interés de la Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A., considerando buenas prácticas y normativas vigentes.

Tabla 2

Nivel de seguridad de grupos de interés

Grupo de Interés	Nivel de Seguridad	Sistema de Tratamiento
Clientes (personas naturales o jurídicas)	Alto	Acceso restringido: Solo personal autorizado puede acceder a datos sensibles y base de datos de cliente Cifrado de datos, políticas de privacidad, cumplimiento legal.
Empleados (Operativos, vendedores, cajeros y administrativos)	Medio	Gestión de personal, Control de accesos de inicio de sesión y permisos diferenciados según el perfil del empleado, Autenticación multifactorial, confidencialidad y actualización de credenciales (cambio de contraseñas y renovación de acceso al dejar el puesto).
Proveedores	Medio	Gestión de compras y relaciones comerciales, Acceso limitado solo personal autorizado puede gestionar información de proveedores, cifrado de comunicaciones, correo, transacciones, auditoría para prevenir fraudes.
Prospectos a empleados	Bajo	Plataforma para recibir, evaluar y gestionar currículos, Confidencialidad de datos personales, acceso restringido solo personal de recursos humanos puede acceder a los CV.
Usuarios de canales digitales	Medio	Recopilación de datos: Formularios, encuestas y sistemas de contacto para captar información de usuarios. Marketing digital: Herramientas para segmentar y personalizar comunicaciones. Cifrado de comunicaciones, protección de datos, gestión de consentimiento de cookies

***Fuente**: Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025.*

Estos sistemas y niveles de seguridad permiten a la empresa gestionar de forma eficiente y segura la información de todos sus grupos de interés, protegiendo la privacidad y asegurando el cumplimiento normativo.

3.2.3. Finalidades, categorías de datos, de interesados y de destinatarios

Tabla 3

Datos de interesados y destinatarios

Grupo de Interesados	Finalidad del Tratamiento	Categorías de Datos	Destinatarios (internos o externos)
Clientes	Gestionar ventas, facturación, entregas, fidelización y comunicaciones comerciales	Nombre, cédula, teléfono, dirección, correo electrónico, historial de compras, método de pago	Área de ventas, contabilidad, bodega.
Empleados	Gestionar la relación laboral, nómina, salud ocupacional, seguridad social y bienestar	Datos de identificación, contacto, datos laborales, financieros, académicos, de salud, y familiares a cargo	Área de talento humano, fondo de pensiones IESS, Ministerio de Trabajo.
Proveedores	Formalizar y gestionar relaciones contractuales, pagos y cumplimiento legal	Datos de contacto, bancarios, RUC, historial comercial	Compras, bancos.
Prospectos a empleo	Evaluación y selección para procesos de contratación	Hoja de vida, datos de contacto, trayectoria académica y laboral, referencias, antecedentes judiciales.	Talento humano, comité de selección
Visitantes	Control de acceso y seguridad en instalaciones	Grabación en CCTV	Recursos Humanos
Contactos comerciales / aliados	Coordinación de actividades comerciales y relaciones estratégicas	Nombre, cargo, correo, teléfono, empresa representada	Gerencia, comercial, Recursos Humanos.
Usuarios digitales (web, redes sociales)	Envío de información, atención de solicitudes, mercadeo y análisis estadístico	Nombre, correo electrónico, intereses, comportamiento de navegación	Marketing.

Fuente: *Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025.*

3.2.4. Encargados de tratamientos

En el contexto de la protección de datos personales, especialmente bajo la LOPDP de Ecuador, existen dos figuras clave en el tratamiento de datos: el responsable del Tratamiento y el Encargado del Tratamiento (Ley Orgánica de Protección de Datos Personales, 2021).

Tabla 4

Encargado de Tratamiento

Encargado	Servicio contratado	Tipo de datos tratados
Empresa de software Confitico)	Gestión comercial: ventas, registro de clientes, facturación, inventario, stock.	Nombres, apellidos, número de identificación, teléfono, dirección, historial de compras.
Empresa de servicios contables (J&S Asesoría contable y tributaria)	Gestión contable y tributaria.	Nombres, RUC, dirección, cuentas bancarias, datos financieros y tributarios.
Proveedor de servicios en la nube (Drive)	Almacenamiento de información y comunicaciones corporativas.	Correos electrónicos, documentos administrativos, datos laborales, datos de contacto.
Empresa de seguridad (Empleados propios)	Videovigilancia y control de ingreso.	Imagen, datos de identificación de visitantes y empleados.

Fuente: *Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025.*

3.3. Registro de Dispositivos (Dispositivos digitales)

Tabla 5

Registro de dispositivos digitales

Área	Tipo de Dispositivo	Uso Principal	Usuario Responsable	Ubicación Física	Nivel de Seguridad Aplicado
Recursos Humanos (RRHH)	PC de escritorio / Laptop	Gestión de hojas de vida, nómina, contratos, afiliaciones	Gerente y jefe de RRHH	Oficina administrativa	Antivirus activo, contraseña individual, acceso restringido, respaldo en la nube
Cajas / Punto de Venta	PC con software impresora.	Facturación, gestión de ventas, cobros con tarjeta	Cajeros(as)	Mostradores de venta	Contraseña por turno, antivirus, datos cifrados, acceso limitado a información sensible

Área	Tipo de Dispositivo	Uso Principal	Usuario Responsable	Ubicación Física	Nivel de Seguridad Aplicado
Atención al Cliente / Recepción	PC / Laptop / Teléfono fijo	Registro de contacto con clientes, agendamiento	Auxiliar de servicio al cliente	Mostrador o zona de atención	Contraseña protegida, sin acceso a datos sensibles, monitoreo de actividad
Bodega / Inventario	Tablet / lector de código de barras / PC	Control de stock, entradas y salidas de producto, reportes de inventario	Auxiliar de bodega / Encargado	Área de almacenamiento	Acceso restringido a inventario, sin conexión a datos personales, conexión interna segura
Ventas Asesores Comerciales	Laptops, celulares corporativos	Atención a clientes, cotizaciones, seguimiento comercial	Asesores internos o externos	Oficinas o trabajo en campo	Aplicaciones protegidas con clave, conexión mediante datos.

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

3.4. Registros de Sistemas de información (Software, seguridad, etc.)

Tabla 6

Registro de Sistemas de información

Nombre del Sistema / Software	Funcionalidad Principal	Tipo de Datos que Trata	Área Responsable	Ubicación / Acceso	Medidas de Seguridad Aplicadas
Correo Electrónico Corporativo (Gmail)	Comunicación interna y con clientes, proveedores	Correo, nombre, mensajes,	Todas las áreas	Web (Gmail)	Doble autenticación, cifrado, control de acceso

		archivos adjuntos			
Sistema CCTV	Vigilancia y monitoreo de instalaciones	Imágenes de empleados, clientes y visitantes	Gerente y RRHH	Instalaciones físicas	Acceso restringido, grabación limitada, borrado periódico
Sitio Web Corporativo redes sociales.	Contacto con clientes, formularios de consulta, cookies	Nombres, correos, mensajes, IPs, cookies	Marketing / Atención cliente	Hosting externo	Certificado de política de privacidad

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

3.5. Registro de personal

3.5.1. Con acceso a Datos

Tabla 7

Registro de personal con acceso a datos

Área / Cargo	Tiene acceso a datos personales	Tipo de datos a los que accede (si aplica)	Medidas de control de acceso
Recursos Humanos	Sí	Datos de empleados (identificación, salud, nómina), candidatos, hojas de vida	Usuario con contraseña, acceso restringido por rol, confidencialidad firmada
Cajas / Punto de venta	Sí	Datos de clientes (nombre, cédula, forma de pago, historial de compras)	Usuario asignado, acceso limitado al sistema POS

Área / Cargo	Tiene acceso a datos personales	Tipo de datos a los que accede (si aplica)	Medidas de control de acceso
Bodega / Inventario	Parcial	Solo acceden a información de productos y logística (no datos personales)	Acceso físico limitado, sin acceso a bases de datos personales
Ventas / Asesores Comerciales	Sí	Datos de clientes (contacto, historial comercial, preferencias)	Acceso con perfil de usuario, contraseña
Gerencia / Dirección	Sí	Acceso total según jerarquía: empleados, clientes, finanzas, contratos	Acceso administrativo a todos los sistemas, confidencialidad firmada

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

3.5.2. Sin acceso a Datos

Tabla 8

Registro de personal sin acceso a datos

Área / Cargo	Tiene acceso a datos personales	Tipo de datos a los que accede (si aplica)	Medidas de control de acceso
Limpieza	No	No accede a datos personales	Ingreso controlado a oficinas, sin acceso a equipos o documentos
Mantenimiento / Técnico	No	No accede directamente a datos personales	Acceso bajo supervisión si requiere trabajar con dispositivos

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

3.5.3. Accesos Físicos

Tabla 9

Accesos físicos

Área o Espacio	Tipo de Información que se Maneja	Personal con Acceso Autorizado	Medidas de Control Físico Implementadas
Oficina de Recursos Humanos	Hojas de vida, contratos, nómina, datos de empleados	Jefe/auxiliar de RRHH, Gerente General	Cerradura con llave, acceso restringido, archivadores bajo llave
Zona de Cajas / Punto de Venta	Datos de clientes (nombre, compras, medio de pago), caja registradora	Cajeros, Supervisor de ventas, Gerente	Cámaras de seguridad, turnos controlados, caja con acceso restringido
Bodega / Almacén	Inventario de productos (no contiene datos personales)	Auxiliares de bodega, jefe de bodega	Candados, acceso autorizado, cámaras
Gerencia / Dirección	Información estratégica, contratos, reportes financieros y personales	Gerente, directivos	Oficina con cerradura, acceso restringido
Área de Servidor o Dispositivos TI (si aplica)	Dispositivos que almacenan información (PC, router, backup externo)	Técnico o personal autorizado	Acceso supervisado, equipos identificados y protegidos
Archivo Físico / Archivadores	Contratos, documentos legales, información de empleados o clientes	RRHH, contabilidad, gerencia	Cerradura con llave, inventario de acceso
Zona común / atención al cliente	No se manejan datos personales directamente	Todo el personal	Libre acceso bajo supervisión, sin documentos expuestos
Área de limpieza y mantenimiento	No acceden a información sensible	Personal externo autorizado	Acceso supervisado, sin llaves ni permisos a oficinas cerradas

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

3.6. Registro de prestadores de servicio

3.6.1. Con acceso a datos catalogados

El registro de prestadores de servicio con acceso a datos catalogados permite identificar a terceros que, en el ejercicio de sus funciones contratadas, pueden acceder parcial o totalmente a información clasificada como **confidencial, sensible o restringida**, conforme a la Ley Orgánica de Protección de Datos Personales.

Tabla 10

Listado

Nombre del prestador de servicio	Tipo de servicio prestado	Tipo de datos a los que accede	Clasificación de los datos
Confitico (Empresa de software)	Sistema de facturación, inventario, clientes	Nombres, RUC, teléfonos, dirección, historial de compras	Confidenciales
Estudio contable (Ej. Asesoría Contable XYZ)	Gestión contable, declaraciones tributarias	Nombres, RUC, ingresos, cuentas bancarias, registros financieros	Confidenciales
Proveedor de hosting y correo electrónico (Ej. Google / Microsoft)	Almacenamiento en la nube y gestión de correos corporativos	Correos electrónicos, archivos adjuntos, documentos internos de la empresa	Confidenciales
Empresa de seguridad (si aplica)	Videovigilancia y control de acceso	Imágenes captadas por cámaras, identificación de visitantes y personal	Sensibles / Confidenciales
Servicio de salud ocupacional (Ej. Médico ocupacional externo)	Evaluaciones médicas, certificados de salud laboral	Resultados médicos, diagnósticos, datos de salud de empleados	Sensibles
Consultor/a externo/a (si aplica)	Asesoría en seguridad, legal, o sistemas de gestión	Información técnica, operativa o personal, dependiendo del alcance del servicio contratado	Confidenciales / Restringidos

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

3.6.2. Sin acceso a datos catalogados

La empresa actualmente no aplica.

3.7. Sistemas de captación de imágenes y audio

El principio de minimización establece que solo se deben recopilar los datos personales que sean adecuados, pertinentes y limitados a lo necesario para las finalidades determinadas, explícitas y legítimas del tratamiento. Este principio busca evitar la recopilación excesiva de información personal, protegiendo así la privacidad y los derechos de las personas (Global Support, 2022).

Justificación de la Grabación de Audio

La grabación de audio en la empresa, al tratarse de un tratamiento de datos personales, debe estar justificada y cumplir con los principios de la LOPDP de Ecuador (Ley Orgánica de Protección de Datos Personales, 2021). Para que la grabación de audio esté justificada, se deben considerar los siguientes aspectos:

1. **Finalidad Legítima y Determinada**
   - Debe existir una finalidad clara y legítima para la grabación de audio (por ejemplo, seguridad, control de calidad, investigación de incidentes).
   - La finalidad debe ser comunicada de manera transparente a las personas afectadas.
2. **Necesidad y Proporcionalidad**
   - La grabación debe ser necesaria para alcanzar la finalidad establecida.
   - Se debe evaluar si existen medios menos invasivos para lograr el mismo objetivo.
3. **Consentimiento Informado**
   - En la mayoría de los casos, se requiere el consentimiento libre, específico, informado e inequívoco de las personas grabadas, salvo que exista una base legal alternativa

(por ejemplo, protección de intereses vitales, cumplimiento de obligaciones legales o interés público).

- El consentimiento debe otorgarse antes de iniciar la grabación y debe poder ser retirado en cualquier momento.

4. **Minimización de Datos**
   - Solo se debe grabar el audio necesario para la finalidad declarada.
   - No se debe grabar más de lo estrictamente necesario y se debe evitar la captura de conversaciones o información irrelevante.
5. **Seguridad y Confidencialidad**
   - Las grabaciones deben estar protegidas contra accesos no autorizados, pérdida o alteración.
   - Se debe establecer un plazo máximo de conservación y garantizar la destrucción segura de las grabaciones una vez cumplida la finalidad (Pro Sciences, 2024)

La empresa mantiene un sistema de CCTV con imagen y audio lo que permite identificar los accesos a las instalaciones.

3.7.1. Número de cámaras

La empresa está equipada con 8 cámaras de audio y video vigilancia la cual se encuentra distribuidas en el área administrativa, cajas, bodegas, zona de corte de madera e ingreso a la empresa y garaje.

3.7.2. Zonas de influencia

Las zonas de influencia esta delimitada por área administrativa, zonas de exhibición de mercadería, bodega, zonas de corte, despacho de mercadería y garaje.

3.7.3. Sistema de tratamiento y almacenamiento

Los sistemas de archivos se distribuyen de manera permanente lo cual se almacena la información en una nube de datos por un tiempo máximo de 30 días.

3.7.4. Usuarios autorizados

Actualmente la alta dirección de la empresa mantiene acceso a la información:

- Gerente general.
- Recursos Humanos.

3.8. Dispositivos Medidas de seguridad

3.8.1. Análisis de las medidas de seguridad de los dispositivos

El análisis de las medidas de seguridad de los dispositivos tiene como finalidad la evaluación y revisión de las medidas de seguridad que se implementaron en los dispositivos con los que cuenta la empresa cuyo propósito es proteger la información y los sistemas contra accesos no autorizados o ataques cibernéticos.

Entre otras medidas preventivas y de seguridad tenemos:

- **Licenciamiento y Actualización de Sistemas Operativos**

Estado: se verifico los sistemas operativos de las computadoras que utiliza la empresa, la organización cuenta con licencias vigentes y legales.

Edición Windows 11 Pro

Versión 24H2

Se instaló el 24/1/2025

Compilación del SO 26100.3775

Experiencia

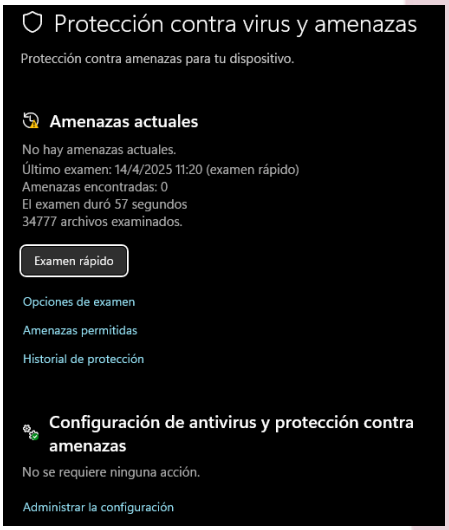
Paquete de experiencia de características de Windows 1000.26100.66.0

- **Licenciamiento y Actualización de Antivirus**

Estado: Confirmar que el antivirus o suite de seguridad instalado en los equipos posea una licencia activa y oficial.

Figura 5

Antivirus



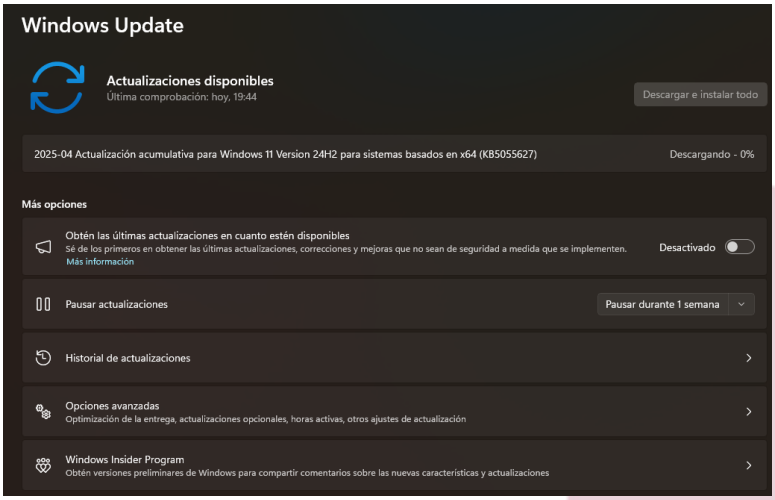
Fuente: *Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025.*

- **Licenciamiento y Actualización de Software**

Estado: Utilizar solo software con licencia válida, evitando el uso de programas piratas o no autorizados.

Figura 6

Actualización de Software



***Fuente**: Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025*

- **Control y Registro de Software Instalado**

  Mantener un inventario actualizado de todo el software instalado, incluyendo licencias, versiones y fechas de renovación.

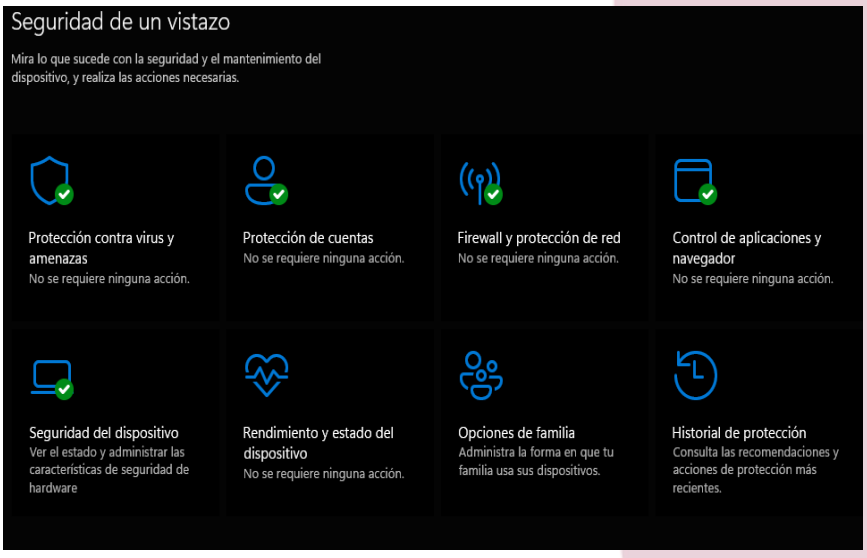
- **Sistemas de Autenticación.** - Permite la verificación de la identidad de los usuarios, así como de los dispositivos con los que se accede a la información y a los sistemas.

- **Sistemas de control y autorización**. – Se basa en roles y permisos que permiten el acceso a la información y a los sistemas.

- **Sistema de cifrado.** – Mediante algoritmos se puede proteger la información cuya finalidad es evitar ser interceptados o intrusiones por terceras personas.
- **Sistemas de detección de intrusos**. – Su misión es detectar y alertar de posibles intrusiones o ataques cibernéticos a la empresa.
- **Sistemas Firewalls**. - Son barreras de seguridad que se crean para controlar el tráfico de red y a la vez generan bloqueos de acceso.
- **Copias de seguridad**. – En el caso de pérdida o daño de la información es indispensable las copias de seguridad de la información o de los sistemas para poder restaurarlos.
- **Actualizaciones de software**. - Periódicamente es necesario la actualización de los sistemas operativos y del software para reducir vulnerabilidades y por ende mejorar las seguridades.

Figura 7

Seguridad del computador



Fuente: *Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025*

3.8.2. Propuesta de mejora de las medidas de seguridad

1. Análisis de Vulnerabilidades: El análisis de vulnerabilidades nos permite identificar y evaluar las vulnerabilidades en los sistemas y dispositivos.

2. Vulnerabilidades de software: Vulnerabilidades en el software y los sistemas operativos que pueden ser explotadas por atacantes.

3. Vulnerabilidades de configuración: Vulnerabilidades en la configuración de los dispositivos y sistemas que pueden ser explotadas por atacantes.

4. Vulnerabilidades de red: Vulnerabilidades en la red que pueden ser explotadas por atacantes.

Algunas de las herramientas que se pueden utilizar para analizar las medidas de seguridad de los dispositivos incluyen:

1. Herramientas de escaneo de vulnerabilidades: Herramientas que escanean los dispositivos y sistemas en busca de vulnerabilidades.

2. Herramientas de análisis de tráfico de red: Herramientas que analizan el tráfico de red para detectar posibles ataques cibernéticos.

3. Herramientas de evaluación de seguridad: Herramientas que evalúan la seguridad de los dispositivos y sistemas.

Lo que nos permite entre otros beneficios:

1. Mejora de la seguridad: Identificación y corrección de vulnerabilidades y debilidades en la seguridad.

2. Reducción del riesgo: Reducción del riesgo de ataques cibernéticos y pérdida de información.

3. Cumplimiento de regulaciones: Cumplimiento de regulaciones y estándares de seguridad.

4. Protección de la información: Protección de la información y los sistemas contra accesos no autorizados y ataques cibernéticos.

3.9. Puestos de trabajo

3.9.1. Análisis de las medidas de seguridad de cada puesto de trabajo, según la información tratada

Los puestos de trabajo se refieren a los cargos o roles que existen dentro de una organización o empresa. A continuación, se presentan algunos ejemplos de puestos de trabajo comunes:

Tabla 11

Análisis de las medidas de seguridad de cada puesto de trabajo

Puesto	Medidas de Seguridad
Operario de corte	Uso de EPP (gafas, guantes, calzado), capacitación en manejo de maquinaria, señalización de zona de riesgo
Vendedor	Orden en mostrador, capacitación en primeros auxilios, protocolos de emergencia Uso de equipo de protección personal: Utilizar equipo de protección personal, como guantes y gafas de seguridad. Manejo seguro de productos: Manejar productos de manera segura para evitar accidentes. Atención al cliente: Atender a los clientes de manera segura y respetuosa
Almacenista	Uso de EPP para manipulación de cargas, señalización de zonas de paso, inspección de mercadería. Uso de equipo de protección personal: Utilizar equipo de protección personal, como guantes y gafas de seguridad. Manejo seguro de productos: Manejar productos de manera segura para evitar accidentes. Organización del almacén: Mantener el almacén organizado y limpio para evitar accidentes.

Puesto	Medidas de Seguridad
Administrativo	Ergonomía en puesto de oficina, capacitación en seguridad informática, protocolos de evacuación
Gerente	Acceso controlado: Restringir el acceso a áreas sensibles de la ferretería. Recibir capacitación en seguridad y salud en el trabajo.

Fuente: *Afines Multitableros & Herrajes S.A., abril, 2025.*

Medidas de Seguridad Generales

1. Señalización de seguridad: Colocar señales de seguridad en áreas de la ferretería donde sea necesario.

2. Iluminación adecuada: Asegurarse de que la iluminación sea adecuada en todas las áreas de la ferretería.

3. Limpieza y organización: Mantener la ferretería limpia y organizada para evitar accidentes.

4. Capacitación en seguridad: Proporcionar capacitación en seguridad y salud en el trabajo a todos los empleados.

Beneficios de las Medidas de Seguridad

1. Prevención de accidentes: Prevenir accidentes y lesiones en el lugar de trabajo.

2. Mejora de la productividad: Mejorar la productividad y eficiencia en el lugar de trabajo.

3. Cumplimiento de regulaciones: Cumplir con las regulaciones y normas de seguridad y salud en el trabajo.

4. Protección de la reputación: Proteger la reputación de la ferretería y mantener la confianza de los clientes.

3.9.2. Acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD DE DATOS DE EMPLEADOS

Entre la Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A. con domicilio en la ciudad de Quevedo, 25 de abril, solar 15 intersección Ángel Zúñiga, representada por el señor Byron López Brito, que, en adelante se denominara "LA EMPRESA", y Álvarez Rodríguez Lourdes Isabel, con domicilio en la ciudad de Quevedo, sector 15 de abril, en adelante denominado "EL EMPLEADO", se conviene en celebrar el presente Acuerdo de Confidencialidad de Datos de Empleados, con el fin de proteger la información confidencial y sensible de la empresa.

1. Datos Identificativos de la Organización

- Nombre legal completo de la empresa: Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A.
- Dirección física y electrónica: ciudad de Quevedo, 25 de abril, solar 15 intersección Ángel Zúñiga, **marketing@multitableros.store**
- Número de identificación fiscal o RUC: 1291767172001
- Datos de contacto (teléfono, correo electrónico): Redes Sociales, Facebook, Instagram, WhatsApp 0985182731.

2. Datos Identificativos del Trabajador

- Nombre completo del empleado: Álvarez Rodríguez Lourdes Isabel
- Número de cédula de identidad: 0623653849
- Cargo o puesto de trabajo: caja
- Datos de contacto (opcional, según necesidad): (+593) 098542793

CLÁUSULA 1: OBJETO DEL ACUERDO

El objeto del presente Acuerdo se establece las condiciones y términos bajo los cuales EL EMPLEADO se compromete a mantener la confidencialidad de los datos y la información de la empresa, así como a no divulgar ni utilizar dicha información para fines distintos a los autorizados por LA EMPRESA.

CLÁUSULA 2: DEFINICIONES

Para los efectos del presente Acuerdo, se entenderá por:

- Información Confidencial: cualquier información, documento, dato o registro que sea considerado confidencial por LA EMPRESA, incluyendo, pero no limitado a, información financiera, comercial, técnica, de marketing, de personal, de clientes, de proveedores, de tecnología, de propiedad intelectual, y cualquier otra información que sea considerada confidencial por LA EMPRESA.
- Datos de Empleados: cualquier información personal, laboral o financiera relacionada con los empleados de LA EMPRESA.

CLÁUSULA 3: OBLIGACIONES DEL EMPLEADO

EL EMPLEADO se compromete a:

- Mantener la confidencialidad de la Información Confidencial y de los Datos de Empleados.
- No divulgar, revelar, copiar, reproducir, transmitir, publicar o utilizar la Información Confidencial o los Datos de Empleados para fines distintos a los autorizados por LA EMPRESA.

- No utilizar la Información Confidencial o los Datos de Empleados para beneficio personal o de terceros.
- Informar a LA EMPRESA de inmediato si tiene conocimiento de cualquier violación o intento de violación de la confidencialidad de la Información Confidencial o de los Datos de Empleados.

CLÁUSULA 4: DURACIÓN DEL ACUERDO

El presente Acuerdo tendrá una **duración indefinida** y permanecerá en vigor aun cuando EL EMPLEADO ya no tenga acceso a la Información Confidencial o a los Datos de Empleados, luego de terminada la relación laboral.

CLÁUSULA 5: LEGISLACIÓN APLICABLE

El presente Acuerdo se regirá e interpretará de acuerdo con las leyes de Ecuador y cualquier disputa o controversia que surja en relación con el mismo será resuelta a través de leyes y códigos vigentes entre esta norma está el art 179 del CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP, 2014)

CLÁUSULA 6: ACUERDO COMPLETO

El presente Acuerdo constituye el acuerdo completo y definitivo entre las partes y sustituye a cualquier acuerdo o entendimiento previo, ya sea verbal o escrito.

CLÁUSULA 7: ACEPTACIÓN

EL EMPLEADO acepta y reconoce que ha leído, entendido y aceptado los términos y condiciones del presente Acuerdo.

Cualquier añadidura o modificación a este acuerdo deberá ser hecha por escrito y firmada por las partes.

CLÁUSULA 8: VIDEOVIGILANCIA

La empresa informa a sus trabajadores que, por motivos de seguridad, las diferentes áreas de trabajo están equipadas con sistemas de videovigilancia, donde las imágenes captadas serán utilizadas netamente para un control interno.

CLÁUSULA 9: USO DE LA IMAGEN DEL TRABAJADOR

La empresa podrá utilizar la imagen de sus trabajadores, solamente con fines institucionales para promocionar o comunicar por medio de redes sociales novedades sobre sus productos. El uso de la imagen de sus trabajadores será respetuoso y con autorización.

SI __ NO__

CLÁUSULA 10: USO DE LOCALIZACIÓN GPS

La empresa informa a sus empleados que algunos dispositivos móviles asignados para las actividades laborales están equipados con sistemas GPS, para garantizar la seguridad y el control adecuado de sus herramientas.

CLÁUSULA 10: EL DERECHOS DEL TRABAJADOR (ARCO)

La empresa comunica a sus trabajadores que pueden ejercer en cualquier momento a sus derechos de acceso, rectificación, cancelación y oposición, establecido en la ley Orgánica de Protección de Datos Personales del Ecuador.

CLÁUSULA 11: DURACIÓN DEL ALMACENAMIENTO DE LOS DATOS DE LOS TRABAJADORES.

La empresa almacena todos los datos más relevantes de los trabajadores en una base de datos, y tendrá una duración de 3, 6, 9 o 12 meses, dependiendo el tiempo de contrato de cada empleado.

Una vez entendido por los comparecientes el contenido y efectos del presente instrumento expresamente se ratifican en él, para fe y constancia se firma el presente documento, en la ciudad de Quevedo a los 8 días del mes de abril del 2025.

Firma de EL EMPLEADO: _____

Firma de LA EMPRESA: _____

Nombre del Representante de LA EMPRESA: Byron Daniel López Brito

Cargo del Representante de LA EMPRESA: Gerente. _____

Es importante que este acuerdo sea revisado y aprobado por un abogado antes de ser firmado.

3.10. Encargado del tratamiento

El encargado del tratamiento se refiere a la persona o entidad responsable de procesar y gestionar los datos personales de los clientes, empleados o proveedores de una organización.

Responsabilidades del Encargado del Tratamiento

1. Gestión de datos: Recopilar, almacenar y procesar los datos personales de manera segura y confidencial.

2. Cumplimiento de regulaciones: Cumplir con las regulaciones y normas de protección de datos personales.

3. Seguridad de la información: Implementar medidas de seguridad para proteger la información personal contra accesos no autorizados.

4. Derechos de los titulares: Respetar y cumplir con los derechos de los titulares de los datos personales, como el derecho a acceder, rectificar y eliminar sus datos.

5. Notificación de incidentes: Notificar a los titulares de los datos personales y a las autoridades competentes en caso de incidentes de seguridad que afecten la confidencialidad, integridad o disponibilidad de los datos.

Funciones del Encargado del Tratamiento

1. Definir políticas de privacidad: Establecer políticas de privacidad y seguridad para el tratamiento de datos personales.

2. Implementar medidas de seguridad: Implementar medidas de seguridad para proteger la información personal.

3. Capacitar al personal: Capacitar al personal sobre la importancia de la protección de datos personales y las políticas de privacidad.

4. Realizar auditorías: Realizar auditorías periódicas para evaluar la eficacia de las medidas de seguridad y cumplimiento de las regulaciones.

5. Responder a solicitudes: Responder a solicitudes de acceso, rectificación y eliminación de datos personales.

3.10. Contrato E. Tratamiento

El contrato del encargado de tratamiento es un acuerdo entre la empresa y el encargado de

tratamiento que establece los términos y condiciones para el tratamiento de los datos personales.

CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS PERSONALES

En la ciudad de Quevedo, a 25 de abril de 2025

REUNIDOS

De una parte, Ferretería Tableros Herrajes & Afines Multitableros & Herrajes S.A., con domicilio en ciudad la de Quevedo, 25 de abril, solar 15 intersección Ángel Zúñiga, y representada por señor Byron López Brito – Gerente General, en adelante, **"El Responsable"**.

De otra parte, CORPORACION NACIONAL DE TELECOMUNICACIONES con domicilio en la Av. 7 de octubre & Calle 13va, y representada por Sr. Paul Santamaria – Gerente General, en adelante, **"El Encargado"**.

Ambas partes, en adelante conjuntamente "las partes", acuerdan celebrar el presente contrato de encargo de tratamiento de datos personales, conforme a lo dispuesto en la normativa vigente en materia de protección de datos, y al tenor de las siguientes cláusulas:

1. OBJETO DEL CONTRATO

El objeto del presente contrato es definir las condiciones conforme a las cuales el Encargado realizará el tratamiento de los datos personales necesarios para la prestación del servicio contratado, siempre bajo las instrucciones del Responsable y en el marco de la normativa aplicable.

2. TIPO DE DATOS Y CATEGORÍAS DE INTERESADOS

El Encargado tendrá acceso a los siguientes tipos de datos personales:

- Nombre y apellidos

- Número de identificación (cédula, DNI, etc.)
- Dirección postal y electrónica
- Teléfono
- Otros datos necesarios para la prestación del servicio (especificar si aplica)
- Las categorías de interesados son: clientes, empleados, proveedores, u otros, según corresponda.

3. FINALIDAD DEL TRATAMIENTO

El tratamiento de los datos personales se realizará exclusivamente para la finalidad de [describir el servicio o finalidad específica], conforme a las instrucciones del responsable.

4. FINALIDAD DEL TRATAMIENTO

El responsable tiene que determinar el grado de afectación de los derechos de los empleados y su naturaleza, como: dirección de vivienda, datos bancarios, etc.

Notificar a la autoridad de protección de datos (dentro de las 72 horas siguientes del incidente) si la vulneración de los datos representa algún tipo de riesgo para los derechos de los empleados.

5. OBLIGACIONES DEL ENCARGADO

El Encargado se obliga a:

- Utilizar los datos personales únicamente para la finalidad acordada y bajo las instrucciones del responsable.
- Garantizar la confidencialidad y seguridad de los datos, implementando las medidas técnicas y organizativas adecuadas.

- No comunicar los datos a terceros, salvo autorización expresa del responsable o exigencia legal.
- Informar inmediatamente al responsable de cualquier incidente de seguridad o vulneración de los datos.
- Permitir auditorías y controles por parte del responsable o autoridades competentes.
- Garantizar que su personal autorizado cumpla con las obligaciones de confidencialidad y protección de datos.

6. SUBCONTRATACIÓN

El Encargado podrá subcontratar total o parcialmente el tratamiento de los datos personales solo con autorización previa, expresa y por escrito del responsable. El subcontratista deberá asumir las mismas obligaciones que el Encargado respecto al tratamiento de los datos.

7. DURACIÓN Y FINALIZACIÓN

El presente contrato tendrá una duración de dos años, prorrogable por acuerdo de las partes. Finalizado el contrato, el Encargado deberá devolver o destruir los datos personales y cualquier soporte que los contenga, salvo obligación legal de conservación.

8. RESPONSABILIDADES

El Encargado será responsable del cumplimiento de las obligaciones establecidas en este contrato y responderá ante el responsable por los daños y perjuicios causados por su incumplimiento.

9. LEGISLACIÓN APLICABLE Y JURISDICCIÓN

El presente contrato se regirá por la legislación de Ecuador, sometiéndose cualquier controversia a los tribunales de Quevedo.

Y en prueba de conformidad, las partes firman el presente contrato por duplicado ejemplar y a un mismo tenor en el lugar y fecha indicados al inicio.

Firma del Responsable	**Firma del Encargado**

3.11. Análisis web

Análisis web y funcionalidad

El sitio web https://www.multitableros.store/ corresponde a la Ferretería Multitableros, un negocio consolidado en el suministro de productos para construcción, hogar y mantenimiento.

- **Tipo de plataforma:** La ferretería ha desarrollado un sistema web progresivo (PWA) de comercio electrónico que permite a los clientes explorar el catálogo, realizar compras en línea y consultar información relevante desde cualquier dispositivo con acceso a internet. Esto mejora la accesibilidad y conveniencia para los usuarios.
- **Herramientas y tecnologías:** El sistema utiliza tecnologías como PHP, Java, HTML5 y bases de datos MySQL, integrando además Power BI para análisis de datos. Esto permite a la ferretería identificar patrones de compra, preferencias de clientes y tendencias de mercado, optimizando la gestión de inventario y la toma de decisiones estratégicas
- **Funcionalidades administrativas:** El sitio incluye herramientas para que los administradores analicen datos comerciales, lo que ayuda a mejorar la competitividad y ampliar el alcance del negocio.

- **Servicios adicionales:** Ofrece asesoría de venta y postventa, envío y entrega inmediata a domicilio, variedad de productos y marcas, garantía de calidad, precios accesibles, pagos directos mediante la aplicación oficial y terminal de cobros para tarjetas de crédito. También cuenta con afiliación y descuentos para compradores frecuentes, lo que agrega valor al cliente.

- **Presencia digital y redes sociales:** La ferretería mantiene presencia en redes sociales como Facebook, Instagram y WhatsApp, facilitando la comunicación con los clientes y soporte directo.

- **Impacto y ventajas competitivas**

  La implementación del sistema PWA e-commerce ha permitido a Ferretería Multitableros adaptarse a las nuevas dinámicas digitales, ampliar su mercado y mejorar la experiencia de compra para sus clientes, quienes ahora pueden acceder a un catálogo actualizado y comprar de forma conveniente desde cualquier lugar.

3.11.1. Análisis, configuración y política de cookies

A continuación, se presenta un análisis de la política de cookies del sitio web multitableros.store, junto con recomendaciones para su implementación y cumplimiento de la normativa ecuatoriana.

1. Presencia y Accesibilidad

Al visitar el sitio web, no se observa un aviso de cookies ni una política de cookies accesible desde la página principal. Esto indica que el sitio no está cumpliendo con las regulaciones que exigen informar y obtener el consentimiento del usuario para el uso de cookies.

2. Tipos de Cookies Utilizadas

Aunque no se dispone de información específica sobre las cookies utilizadas por el sitio, es probable que se empleen cookies esenciales para el funcionamiento del sitio, así como cookies de análisis y de terceros para publicidad y seguimiento.

Estas cookies deben ser identificadas y clasificadas adecuadamente en una política de cookies.

Implementación de una Política de Cookies

1. Elaboración de una Política de Cookies Transparente

Es fundamental crear una política de cookies clara y accesible que detalle:

- **Definición de Cookies**: Explicar qué son las cookies y su propósito.
- **Tipos de Cookies**: Clasificar las cookies utilizadas según la finalidad (técnicas, analíticas, publicitarias, etc.).
- **Cookies de Terceros**: Informar sobre la utilización de cookies de terceros y sus finalidades.
- **Consentimiento del Usuario**: Indicar cómo se obtiene el consentimiento del usuario para el uso de cookies.
- **Gestión de Cookies**: Instrucciones sobre cómo el usuario puede gestionar o eliminar las cookies en su navegador

2. Implementación de un Banner de Consentimiento

Al acceder al sitio de la empresa, no se muestra un banner que informe al usuario sobre el uso de cookies y/o solicitud de su consentimiento antes de instalar cookies para continuar navegando por

la página web. Este banner no permitir al usuario aceptar o configurar el uso de cookies y acceder a la política de cookies completa.

3. Configuración de Preferencias de Cookies

El sitio debe ofrecer una herramienta que permita al usuario configurar sus preferencias de cookies, aceptando o configurando categorías específicas según su elección.

4. Cumplimiento de la Normativa Ecuatoriana

La política de cookies debe cumplir con la **Ley Orgánica de Protección de Datos Personales (LOPDP)** de Ecuador, que establece la obligación de informar y obtener el consentimiento del usuario para el tratamiento de sus datos personales, incluyendo el uso de cookies.

3.11.2. Formularios de contacto, newsletter, trabaja conmigo, registro

Según la información disponible, el sitio web multitableros.store, cuenta con un formulario de contacto para atención al cliente y soporte.

No se evidencia un formulario visible para newsletter o suscripción por correo.

No hay sección pública clara para “Trabaja con nosotros” ni para registro de usuarios, aunque podrían estar disponibles en áreas internas o mediante contacto directo. Todos los formularios deben cumplir con normativas de privacidad y seguridad para proteger los datos de los usuarios.

Se presentan formularios efectivos en el sitio web, para los formularios de contacto, suscripción a newsletters, postulación a empleos y registro de usuarios.

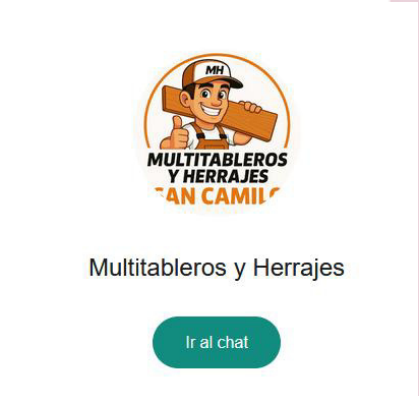
1. Formulario de Contacto

Objetivo: Facilitar la comunicación directa entre los usuarios y la empresa de Ferretería Multitableros.

- **Campos esenciales:** Nombre, correo electrónico y mensaje.
- **Diseño responsivo:** Asegura que el formulario se vea correctamente en dispositivos móviles y de escritorio.
- **Validación en tiempo real:** Informa al usuario sobre errores en los campos mientras completa el formulario.
- **Política de privacidad:** Incluye un enlace a tu política de privacidad y una casilla para que el usuario acepte el tratamiento de sus datos.

Figura 8

Formato de contacto



***Fuente**: Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025*

2. Formulario de Suscripción al Newsletter

Objetivo: Captar correos electrónicos para enviar actualizaciones, promociones o contenido relevante.

- **Campos mínimos:** Solicita solo el correo electrónico; la simplicidad aumenta las conversiones.
- **Claridad en el propósito:** Indica claramente qué tipo de contenido recibirá el usuario y con qué frecuencia.
- **Confirmación de suscripción:** Implementa un sistema de doble opt-in para verificar la autenticidad del correo electrónico.
- **Enlace a la política de privacidad:** Asegura que los usuarios sepan cómo se utilizarán sus datos.

Figura 9

Suscripción

***Fuente**: Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025*

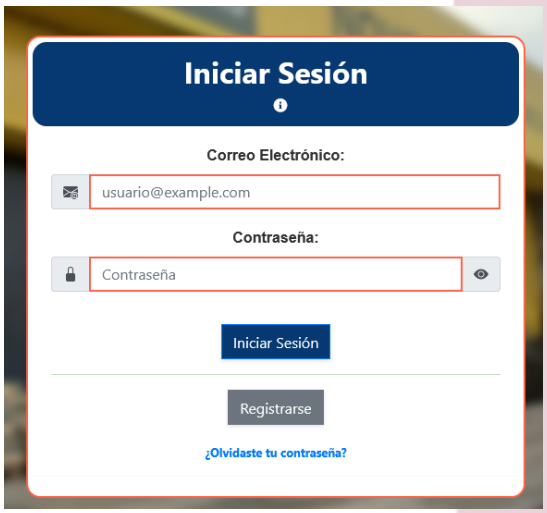
3. Formulario de Registro de Usuario

Objetivo: Permitir que los usuarios creen una cuenta en tu sitio para acceder a servicios personalizados.

- **Campos esenciales:** Nombre, correo electrónico y contraseña.
- **Contraseña segura:** Requiere una contraseña con una combinación de letras, números y caracteres especiales.
- **Confirmación de correo electrónico:** Envía un correo de verificación para confirmar la autenticidad del registro.
- **Texto legal:** Incluye una casilla para que el usuario acepte los términos y condiciones y la política de privacidad.

Figura 10

Registro de Usuario



***Fuente**: Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025*

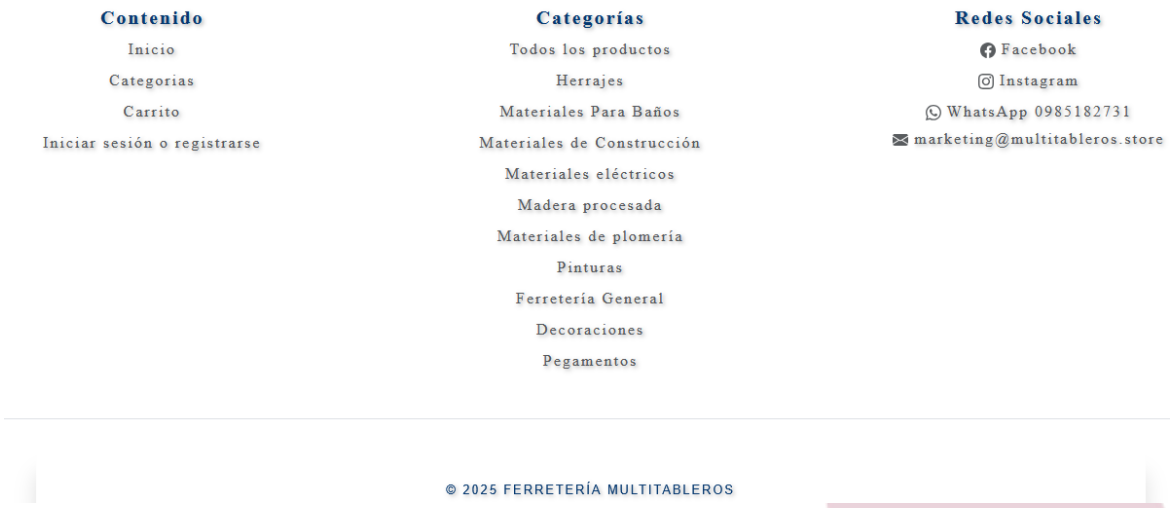
4. Formulario "Trabaja con Nosotros"

Objetivo: Permitir que los candidatos postular a ofertas de empleo disponibles en la empresa Ferretería Multitableros.

- **Campos esenciales:** Nombre, correo electrónico, posición de interés y adjunto (CV).
- **Descripción clara:** Indica claramente qué tipo de perfil estás buscando y qué documentos son necesarios.
- **Confirmación de recepción:** Envía un correo electrónico automático confirmando la recepción de la postulación.
- **Enlace a la política de privacidad:** Informa a los postulantes cómo se manejarán sus datos personales

Figura 11

No dispone el link para CV



***Fuente**: Empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., abril, 2025*

Formulario de Compra

Objetivo:

Facilitar la recolección de datos personales y de contacto de los clientes con el fin de gestionar adecuadamente las órdenes de compra realizadas a través de canales físicos o digitales.

Campos esenciales:

Nombres y apellidos

Número de identificación (cédula o RUC)

Dirección de entrega

Número telefónico

Correo electrónico

Detalle de productos solicitados

Forma de pago

Descripción clara:

El formulario indica de manera visible los datos requeridos para procesar correctamente la compra, facturar y coordinar la entrega del pedido. También especifica que estos datos serán utilizados exclusivamente para fines comerciales, conforme a la normativa legal vigente.

Confirmación de recepción:

El sistema genera una confirmación automática de la compra, ya sea mediante correo electrónico o comprobante físico/digital, que incluye el número de orden y los datos del cliente.

Enlace a la política de privacidad:

El formulario incluye un aviso de privacidad que informa al cliente sobre el tratamiento de sus datos personales, así como un enlace directo al documento completo de la política de privacidad publicada en el sitio web o disponible en formato físico en el punto de venta.

3.11.3. Avisos Legales

En el sitio web multitableros.store, No se encontró resultados, página o documento específico que contenga el Aviso Legal formal.

Como mejora se sugiere crear Aviso Legal para la Ferretería Multitableros en los siguientes aspectos:

- **Titularidad del sitio:** El sitio es propiedad privada y está operado por Ferretería Multitableros, ubicada en el Cantón Quevedo, provincia de Los Ríos, Ecuador.
- **Objeto:** El sitio web ofrece un sistema PWA de comercio electrónico para la venta de materiales de construcción, herramientas, herrajes, pinturas, y otros productos relacionados con ferretería.
- **Propiedad intelectual:** Los contenidos, imágenes, marcas y diseños del sitio son propiedad de Ferretería Multitableros o sus proveedores y están protegidos por la legislación vigente.

- **Responsabilidad:** La Ferretería Multitableros se compromete a mantener la información actualizada, pero no se responsabiliza por errores, interrupciones o daños derivados del uso del sitio.
- **Protección de datos:** Aunque no se encontró una política específica, se recomienda que el sitio incluya un apartado sobre la protección de datos personales conforme a la normativa ecuatoriana y otras aplicables, informando sobre la recopilación, uso y tratamiento de datos de clientes y usuarios.
- **Condiciones de uso:** El usuario se compromete a utilizar el sitio para fines lícitos y a respetar los derechos de propiedad intelectual y las normas de conducta.
- **Jurisdicción:** Cualquier controversia derivada del uso del sitio se someterá a la legislación y tribunales de Ecuador.

3.12. Medidas de seguridad

3.12.1. Análisis, uso y medidas de seguridad en el uso de navegadores

Los navegadores web son herramientas primordiales y ahora parte esencial en cualquier entorno empresarial, para el caso de nuestra empresa no es la excepción, ya que permiten el acceso a sistemas de gestión, tiendas en línea, proveedores y otros servicios críticos. Sin embargo, por las múltiples funciones que se le da a esta herramienta también son una de las principales vías de ataque para los ciberdelincuentes. A continuación, describimos las principales vulnerabilidades y riesgos relacionados con los navegadores web que más se utiliza en la empresa:

Vulnerabilidades específicas de los navegadores que se usan con más frecuencia en la empresa

Google Chrome

- **Riesgo:** Si bien es uno de los navegadores más seguros, su popularidad lo convierte en un objetivo principal para los atacantes.
- **Problemas comunes:**
    - Extensiones maliciosas.
    - Vulnerabilidades en su motor Blink.
    - Rastreo excesivo de datos por parte de terceros.

Mozilla Firefox

- **Riesgo:** Aunque es conocido por su enfoque en la privacidad, puede ser vulnerable si no se actualiza regularmente.
- **Problemas comunes:**
    - Vulnerabilidades en su motor Gecko.
    - Menor compatibilidad con algunos estándares de seguridad modernos.

Vulnerabilidades comunes en navegadores web que se usan con mayor frecuencia en la empresa

a. Extensiones maliciosas o inseguras

- **Riesgo:** La empresa utiliza extensiones para optimizar la funcionalidad de los diferentes navegadores (por ejemplo, para gestionar contraseñas o bloquear anuncios). Sin embargo, algunas de estas pueden contener códigos maliciosos o no estar debidamente actualizadas, lo que las convierte en un instrumento dañino que puede atacar a nuestro sistema.

- **Impacto:** Robo de datos confidenciales, como credenciales o información financiera.

b. Fallas en el motor del navegador

- **Riesgo:** Los navegadores tienen motores de renderizado (como Blink en Chrome o Gecko en Firefox) que pueden contener vulnerabilidades. Estas fallas pueden ser explotadas por atacantes para ejecutar código malicioso.
- **Impacto:** Ejecución remota de código, instalación de malware o ransomware.

c. Ataques a través de JavaScript

- **Riesgo:** El lenguaje JavaScript es ampliamente utilizado en aplicaciones web, pero también puede ser explotado para realizar ataques como **cross-site scripting (XSS)**.
- **Impacto:** Los atacantes pueden inyectar scripts maliciosos en sitios web legítimos, lo que puede comprometer la seguridad de los datos de los usuarios.

d. Falta de actualizaciones

- **Riesgo:** Si los navegadores no están actualizados, pueden ser vulnerables a fallas conocidas que ya han sido parcheadas en versiones más recientes.
- **Impacto:** Exposición a ataques debido a vulnerabilidades conocidas.

Principales riesgos asociados al uso de navegadores que se usan con mayor frecuencia en la empresa

a. Phishing

- **Riesgo:** Los empleados pueden ser engañados para acceder a sitios web falsos que imitan a proveedores, bancos u otros servicios esenciales.

- **Impacto:** Robo de credenciales, pérdida de acceso a cuentas críticas o transferencia de dinero a cuentas fraudulentas.

b. Descarga de archivos maliciosos

- **Riesgo:** Al descargar catálogos, facturas o software desde sitios web no confiables, los usuarios pueden instalar malware sin darse cuenta.
- **Impacto:** Infección del sistema con ransomware, spyware o troyanos.

c. Ataques de hombre en el medio (MITM)

- **Riesgo:** En redes Wi-Fi públicas o mal configuradas, un atacante puede interceptar la comunicación entre el navegador y el servidor.
- **Impacto:** Robo de datos, manipulación de comunicaciones o instalación de malware.

d. Cookies de sesión y rastreo

- **Riesgo:** Las cookies almacenan información sobre las sesiones de los usuarios. Si no están protegidas, pueden ser robadas mediante ataques como **session hijacking**.
- **Impacto:** Acceso no autorizado a cuentas empresariales o sistemas internos.

e. Configuraciones de seguridad débiles

- **Riesgo:** Configuraciones por defecto o mal ajustadas (como permitir el uso de contenido mixto HTTP/HTTPS) pueden exponer a los usuarios a ataques.
- **Impacto:** Pérdida de datos o infecciones de malware.

Recomendaciones para mitigar riesgos

1. **Mantener navegadores actualizados:** Configurar actualizaciones automáticas para garantizar que las vulnerabilidades conocidas sean parcheadas.

2. **Usar extensiones confiables:** Limitar el uso de extensiones solo a aquellas provenientes de fuentes verificadas.
3. **Implementar soluciones de seguridad adicionales:**
    - Antivirus y antimalware.
    - Firewalls empresariales.
    - Navegación segura (HTTPS en todos los sitios).
4. **Capacitar al personal:** Educar a los empleados sobre los riesgos de phishing, descargas no seguras y sitios web sospechosos.
5. **Configurar políticas de seguridad:** Restringir el acceso a sitios web no relacionados con la actividad empresarial.
6. **Hacer auditorías de seguridad periódicas:** Revisar configuraciones de seguridad y realizar pruebas de penetración para identificar vulnerabilidades.

3.12.2. Hosting y Servidores

Para la empresa según el tamaño, el volumen de tráfico esperado en su página web, los servicios que desean ofrecer (e-commerce, catálogos en línea, sistemas de gestión internos, etc.) y su presupuesto. Presentamos las opciones más recomendadas:

1. Características clave que debe tener el hosting para la empresa

Importante considerar las siguientes características:

a. Rendimiento y velocidad

- **Importancia:** La página web debe cargar rápido, especialmente si incluye un catálogo de productos o una tienda en línea.
- **Recomendación:** Optar por hosting con discos SSD, servidores optimizados y CDN (Red de Distribución de Contenidos) para mejorar la velocidad de carga.

b. Escalabilidad

- **Importancia:** Si la empresa crece o el tráfico aumenta, el hosting debe poder adaptarse sin interrupciones.
- **Recomendación:** Hosting escalable, como servidores en la nube o VPS (servidores virtuales privados).

c. Soporte para e-commerce

- **Importancia:** Si la empresa tiene una tienda en línea, el hosting debe ser compatible con plataformas como WooCommerce, Shopify, Magento o PrestaShop.
- **Recomendación:** Hosting con certificación SSL, integración con pasarelas de pago y soporte para bases de datos robustas.

d. Seguridad

- **Importancia:** El sitio web debe estar protegido contra ataques cibernéticos, como malware, phishing o DDoS.
- **Recomendación:** Hosting con firewalls, protección contra DDoS, copias de seguridad automáticas y certificados SSL.

e. Facilidad de uso

- **Importancia:** Si la empresa no cuenta con un equipo técnico, el hosting debe ofrecer paneles de control fáciles de usar, como cPanel o Plesk.
- **Recomendación:** Hosting con soporte técnico 24/7 y documentación clara.

2. Tipos de hosting recomendado para la empresa

a. Hosting compartido

- **Ideal para:** Empresas pequeñas con sitios web básicos, como catálogos de productos o páginas informativas.
- **Ventajas:**
  - Económico.
  - Fácil de configurar.
- **Desventajas:**
  - Recursos limitados.
  - Menor seguridad y rendimiento.
- **Ejemplo de proveedores:**
  - **Bluehost**.
  - **HostGator**.

3. Mejores proveedores de hosting y servidores para la empresa

a. Bluehost

- **Por qué elegirlo:** Ideal para pequeñas y medianas empresas con sitios web en WordPress.
- **Características destacadas:**
  - Integración fácil con WooCommerce.

- Precios accesibles.
- Dominio gratuito el primer año.

b. HostGator

- **Por qué elegirlo:** Una opción económica para empresas pequeñas.
- **Características destacadas:**
  - Planes accesibles.
  - Fácil de usar.
  - Buen soporte técnico.

4. Recomendación final según el tamaño de la empresa

- **Empresas pequeñas:**
  - Hosting compartido o VPS (ejemplo: Bluehost, SiteGround).
  - Ideal para catálogos simples o páginas informativas.

En base de las necesidades específicas planteamos los lineamientos priorizando la seguridad, el rendimiento y la escalabilidad.

3.12.2.1. Medidas de seguridad

Principales medidas de seguridad para un sitio web

1. Implementar HTTPS (SSL)

- Asegura la comunicación entre el navegador del usuario y el servidor.
- Evita que terceros intercepten datos (como formularios o contraseñas).
- Obliga a redirigir todo el tráfico de HTTP a HTTPS.

2. Realizar copias de seguridad periódicas

- Backups diarios o semanales de archivos, bases de datos y configuraciones.
- Almacenarlos en ubicaciones externas (cloud o servidores independientes).
- Verificar que los backups se restauren correctamente.

3. Actualizar software y plugins

- Mantener siempre actualizados:
- CMS (como WordPress, Joomla)
- Plugins o módulos externos
- Librerías JavaScript y temas
- Las actualizaciones corrigen vulnerabilidades conocidas.

4. Protección de formularios

- Validación del lado cliente y servidor.
- Uso de CAPTCHA o reCAPTCHA (para evitar bots y spam).
- Limitar intentos de envío para prevenir ataques por fuerza bruta.

5. Uso de firewalls (WAF)

- Un **Web Application Firewall** bloquea tráfico malicioso antes de que llegue al servidor.
- Protege contra ataques XSS, inyecciones SQL, etc.

6. Control de accesos

- Contraseñas seguras (mínimo 12 caracteres, con letras, números y símbolos).
- Activar autenticación en dos pasos (2FA) para administradores.
- Limitar accesos por IP o roles específicos.

7. Monitoreo y detección de intrusos

- Herramientas como **Sucuri**, **Wordfence**, **MalCare** o **SiteLock** escanean el sitio buscando malware o accesos sospechosos.
- Usar sistemas de log para detectar accesos inusuales al panel de administración.

8. Gestión segura de cookies

- Usar el atributo Secure, HttpOnly y SameSite=Strict en cookies.
- Implementar una política clara de cookies con consentimiento explícito si usas analítica o publicidad.

10. Evitar almacenamiento innecesario de datos personales

- No almacenar información sensible (como tarjetas de crédito) en el servidor sin necesidad.
- Cumplir la **Ley Orgánica de Protección de Datos Personales (LOPDP)** de Ecuador.

3.12.2.2. Prestadores de servicios

Cuando hablamos de **prestadores de servicios** en el contexto del sitio web de Ferretería Multitableros, nos referimos a todas las empresas o profesionales que participan directa o indirectamente en su funcionamiento, seguridad, diseño y crecimiento.

Tipos de Prestadores de Servicios para un Sitio Web

1. Servicios de Hosting y Dominio

Empresas que alojan tu sitio web y gestionan tu nombre de dominio.

- **GoDaddy**, **Hostinger**, **SiteGround** – alojamiento web.
- **Google Domains**, **Namecheap** – registro de dominios.

- **Cloudflare** – DNS, firewall y CDN.

2. Diseño y desarrollo web

Especialistas en crear o personalizar el sitio:

- **Diseñadores web** (UX/UI)
- **Desarrolladores Frontend/Backend** (HTML, CSS, JavaScript, PHP, etc.)
- **Agencias digitales** o freelancers especializados en eCommerce o CMS como WordPress, Shopify, etc.

3.12.3. Gestores de Correo electrónico

Tipos de Gestores de Correo Electrónico (Webmail / Online)

Accedes a través del navegador, sin instalar software.

Tabla 12

Gestores de Correo electrónico

Gestor	Características
Gmail (Google Workspace)	Profesional, filtros avanzados, excelente antispam.
Outlook (Microsoft 365)	Integrado con Office, buena para empresas.
Zoho Mail	Buena opción gratuita para dominios propios.
ProtonMail	Enfocado en privacidad y cifrado.
Roundcube / Horde	Comunes en servicios de hosting compartido.

Fuente: *https://www.softwaredoit.es/software-comunicacion/gestor-correo-electronico-email.html, abril, 2025.*

3.12.3.1. Medidas de seguridad

1. Autenticación segura

- **Contraseñas fuertes**: mínimo 12 caracteres, mezclando mayúsculas, números y símbolos.

- **Autenticación de dos factores (2FA)**: protección extra al iniciar sesión desde un nuevo dispositivo.

- Gmail: Google Authenticator o código SMS.
- Outlook: Microsoft Authenticator.
- Zoho: Zoho OneAuth.

2. Encriptación de los correos

- **Encriptación en tránsito (TLS)**: protege los mensajes mientras se envían entre servidores.
- **Encriptación de extremo a extremo (E2EE)**: el contenido solo puede ser leído por el remitente y el destinatario.

- Usado por ProtonMail, Tutanota o extensiones como Mailvelope (PGP para Gmail/Outlook).

3. Protección contra suplantación (phishing y spoofing)

A través de registros DNS configurados en el dominio:

Tabla 13

Protección contra suplantación

Registro	Función
SPF	Especifica qué servidores pueden enviar correos desde tu dominio.
DKIM	Firma criptográficamente tus correos para validar su autenticidad.
DMARC	Reglas de verificación para SPF y DKIM; notifica intentos de suplantación.

Fuente: *https://www.sophos.com/es-es/products/sophos-email. abril, 2025.*

4. Filtros antispam y antivirus

- Todos los gestores modernos (Gmail, Outlook, Zoho) filtran correos sospechosos y contienen bases de datos de malware conocidas.
- Recomendado: no abrir adjuntos de fuentes desconocidas ni hacer clic en enlaces sin verificar.

5. Control de dispositivos y sesiones

- Permite cerrar sesiones remotas desde el panel de control.
- Gmail y Outlook muestran los dispositivos conectados, ubicación y hora.
- Zoho y ProtonMail permiten bloquear accesos inusuales automáticamente.

6. Protección contra acceso no autorizado

- Limitar intentos fallidos (bloqueo por fuerza bruta).
- Bloqueo geográfico o por IP.
- Control de acceso por aplicación (OAuth2 y permisos granulares).

7. Auditoría y registros de actividad (logs)

- Google Workspace y Microsoft 365 ofrecen paneles de seguridad con:
- Alertas de actividad sospechosa.
- Registros de acceso, envío y recepción.
- Recomendado en entornos empresariales.

3.12.3.2. Prestadores de servicios

Prestadores de servicios de correo electrónico (con dominio propio)

1. Google Workspace (antes G Suite)

- Dominio personalizado: tu-nombre@tudominio.com
- Almacenamiento: 30 GB a 5 TB según plan
- Integración: Gmail + Drive + Meet + Calendar
- Seguridad: 2FA, filtros avanzados, cumplimiento GDPR/LOPDP
- Desde $6 USD/usuario/mes

2. Microsoft 365 (Outlook Business)

- Correo empresarial con @tudominio.com
- Integra Outlook, Word, Excel, Teams
- Alta seguridad corporativa y cifrado
- Desde $6 USD/usuario/mes

3. Zoho Mail

- Plan gratuito para hasta 5 usuarios con dominio personalizado
- Interfaz moderna, buen soporte y privacidad
- Sin publicidad, buen antispam
- Desde $0 a $3 USD/usuario/mes

4. ProtonMail (ahora Proton Mail for Business)

- Enfoque en privacidad y cifrado de extremo a extremo
- Servidores en Suiza
- Interfaz moderna, aunque más limitada en funciones empresariales

- Desde $3.99 USD/usuario/mes

5. Titan Mail (ofrecido por Hostinger, Namecheap, etc.)

- Profesional, ligero, ideal para pymes
- App móvil, firmas automáticas y bandeja limpia
- Integra fácilmente con dominios desde Hostinger
- Desde $1.50 USD/usuario/mes

CAPITULO 4

CONFECCIÓN DE UN PLAN DIRECTOR DE SEGURIDAD

4. DESCRIPCIÓN DE LO QUE ES UN PLAN DIRECTOR DE SEGURIDAD Y LOS BENEFICIOS PARA LA EMPRESA

La seguridad corporativa es un componente esencial para el funcionamiento eficiente y sostenible de una empresa. En el caso de Multi Tableros & Herrajes, cuya operación involucra materiales inflamables, manejo de inventario de alto valor y exposición a riesgos internos y externos, es fundamental establecer un plan de seguridad integral.

Este documento presenta el Plan de Seguridad Corporativa diseñado para proteger los activos físicos, tecnológicos y humanos de la organización. Incluye estrategias preventivas, análisis de vulnerabilidades y protocolos de acción frente a amenazas como incendios, robos, ciberataques, y riesgos personales a empleados y directivos.

El objetivo de este plan es **garantizar la protección de los bienes, personas e información de Multi Tableros & Herrajes**, a través de la implementación de políticas, procedimientos y herramientas que mitiguen los riesgos operacionales y fortalezcan la resiliencia de la organización ante eventos adversos.

4. 1. Check List PDS

Tabla 14

Check List

N	NIVEL	ALCANCE	CONTROL	
1	B	PRO	¿Existe una política de seguridad de la información documentada y aprobada?	☒
2	B	PRO	¿La política de seguridad se revisa periódicamente?	☐
3	B	PER	¿Se han definido y comunicado las responsabilidades en materia de seguridad?	☒
4	A	PRO	¿Existe un Comité de Seguridad encargado de la gestión de seguridad de la información?	☐
5	B	PRO	¿Los contratos con terceros incluyen cláusulas de seguridad (confidencialidad, propiedad, etc.)?	☐
6	B	TEC	¿Se dispone de un inventario actualizado de activos?	☒
7	B	PRO	¿Se ha definido el responsable de cada activo?	☒
8	B	PRO	¿Se comprueban las referencias de los candidatos a empleo?	☐
9	B	TEC	¿Existen perímetros de seguridad física (accesos controlados, cámaras, etc.)?	☒
10	A	TEC	¿Los equipos TIC críticos están ubicados en salas seguras?	☐
11	A	TEC	¿Se han documentado los procedimientos operativos TIC?	☐
12	B	TEC	¿Se realizan copias de seguridad regularmente?	☒
13	B	TEC	¿Se verifica la correcta realización de las copias de seguridad?	☒
14	A	TEC	¿Se monitoriza y registra la actividad de los equipos críticos?	☐
15	A	TEC	¿Se registran las actividades de los administradores de sistemas?	☐
16	B	TEC	¿Existe una sistemática para la asignación y uso de privilegios en los sistemas?	☐
17	B	TEC	¿Se han definido procedimientos formales para la gestión de contraseñas?	☐

18	B	PER	¿Se exige a los usuarios buenas prácticas en el uso de contraseñas?	☒
19	B	PER	¿Se protege el acceso a equipos desatendidos (bloqueo, cierre de sesión)?	☐
20	B	TEC	¿Las cuentas de usuario son unipersonales?	☒
21	B	TEC	¿Se controla la instalación de software en sistemas en producción?	☐
22	A	TEC	¿Existe un proceso para la gestión de vulnerabilidades técnicas?	☐
23	A	PRO	¿Se ha documentado un proceso para la gestión de incidentes de seguridad?	☐
24	A	PRO	¿Existe un plan de continuidad de negocio documentado?	☐
25	A	PRO	¿Se revisan y prueban los planes de continuidad de negocio?	☐
26	B	PRO	¿Se identifican y cumplen los requisitos legales relevantes?	☒
27	B	PRO	¿Existen procedimientos para asegurar el cumplimiento de requisitos legales?	☒
28	A	PRO	¿Se han establecido procedimientos para la protección y privacidad de la información?	☐
29	A	TEC	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a estándares?	☐

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Diagnóstico inicial

Objetivo: Identificar los activos, amenazas y vulnerabilidades clave de la empresa.

a. Activos Críticos:

- **Personas:** Empleados, directivos
- **Infraestructura:** Local comercial, oficinas

- **Equipos y sistemas:** CCTV, computadoras, software de inventario
- **Información:** Inventarios, datos contables, datos personales de empleados, clientes y proveedores
- **Productos:** Herrajes y tableros de madera (material inflamable)

b. Amenazas:

- Incendios por materiales inflamables
- Robo externo (intrusos)
- Robo interno (empleados)
- Ciberataques o pérdida de información
- Secuestros y extorsiones a empleados o directivos

c. Vulnerabilidades detectadas:

Tabla 15

Vulnerabilidad y Consecuencia

Área	Vulnerabilidad Detectada	Consecuencia
Accesos físicos	Puertas sin refuerzo o control riguroso	Robo externo
Almacenamiento	Material inflamable sin medidas especiales	Incendios
Seguridad interna	Posible complicidad o negligencia de empleados	Robo interno
Tecnología	Ausencia de firewall, backup y antivirus profesional	Ciberataques, pérdida de datos

Gestión	No hay protocolos ante secuestros/extorsión	Alta exposición a amenazas personales

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Evaluación de Riesgos

Se analiza el **impacto** (I) y la **probabilidad** (P) para establecer el nivel de riesgo (R):

Tabla 16

Análisis Impacto vs Probabilidad para establecer el nivel de riesgo

Riesgo	I (1–5)	P (1–5)	R = I × P	Nivel de Riesgo
Incendio	5	4	20	Crítico
Robo externo	4	3	12	Alto
Robo interno	3	4	12	Alto
Secuestro/extorsión	5	2	10	Alto
Ciberataque	5	4	20	Crítico
Pérdida de inventario por fallo informático	4	3	12	Alto

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Interpretación: Riesgos como **incendios** y **ciberataques** deben priorizarse inmediatamente, seguidos por robos y amenazas personales.

Diseño de Medidas de Seguridad

Se definen medidas **preventivas**, **disuasorias**, **reactivas** y de **recuperación**.

a.- Preventivas:

- Implementar control de accesos (lectores biométricos o tarjetas)
- Asegurar almacenamiento de materiales inflamables con señalética y extintores adecuados

- Antivirus, firewall y backups automáticos
- Protocolos de seguridad para empleados y capacitación

b.- Disuasorias:

- Cámaras visibles en puntos clave, asegurando sin puntos ciegos
- Alarmas perimetrales activadas fuera del horario laboral
- Letreros visibles que indiquen vigilancia y protocolos de emergencia

c.- Reactivas:

- Plan de evacuación ante incendios
- Protocolo de respuesta ante intrusión o robo
- Comunicación inmediata con policía o bomberos
- Plan de contingencia en caso de ataque informático

d.- Recuperación:

- Respaldos de datos cada 24 horas en la nube
- Seguro empresarial contra incendio y robo
- Revisión de inventario con bitácora digital y copia de seguridad

Implementación

Tabla 17

Fase práctica del plan de seguridad

Área	Acción	Responsable	Recursos
Acceso físico	Instalar cerraduras reforzadas y cámaras adicionales	Encargado de seguridad	USD 500
Riesgo de incendio	Señalética, extintores tipo ABC, ruta de evacuación	Supervisor de almacén	USD 700
Ciberseguridad	Firewall, antivirus, backups automáticos	Técnico informático	USD 300
Seguridad personal	Crear protocolo para amenazas y capacitar personal	Gerente RH + Policía	Coordinación
Inventario	Software actualizado con alertas de errores	Encargado TI	Software ERP o similar

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Seguimiento y Mejora Continua

a.- Para mantener el plan vigente y efectivo:

- **Auditorías internas mensuales:** revisión de cámaras, accesos, inventario
- **Simulacros bimensuales:** evacuación, intrusión, fuga de datos
- **Revisión de seguridad informática:** cada 3 meses, con logs y verificación de respaldos
- **Encuestas de percepción de seguridad:** semestrales para los empleados

- **Actualización del plan:** anual, según cambios operacionales o incidentes.

4.1.1. Análisis de la situación actual de la empresa

Control de accesos físicos y digitales

Situación actual:

- La empresa tiene **2 puertas de ingreso** sin control electrónico visible.
- No se menciona el uso de credenciales, tarjetas o control digital para accesos.

Análisis:

- El control físico debe reforzarse con **puertas con cerraduras electrónicas** o tarjetas magnéticas.
- Se recomienda una bitácora digital de entrada/salida de personal y visitas.
- A nivel digital, se deben **proteger accesos a software** e inventario con contraseñas seguras y acceso restringido.

Riesgos mitigados:

- Robos internos y externos
- Infiltraciones
- Sabotaje o fuga de información

Revisión y mantenimiento del sistema de videovigilancia y alarmas

Situación actual:

- 8 cámaras de videovigilancia y sistema de alarma instalados.

Análisis:

- Evaluar si existen **puntos ciegos** o cámaras que requieren actualización (resolución, visión nocturna).
- Verificar **grabación continua y almacenamiento seguro** de los videos (idealmente, en la nube).
- Las alarmas deben conectarse a servicios de respuesta rápida o seguridad privada.
- Se sugiere un **plan de mantenimiento trimestral**.

Riesgos mitigados:

- Robo externo
- Accesos no autorizados
- Incidentes sin registro de evidencia

Plan de respuesta ante incendios y evacuación

Situación actual:

- Material inflamable (tableros y químicos de ferretería).

Análisis:

- El riesgo de incendio es crítico. Se debe implementar:
  - ✓ **Detectores de humo**
  - ✓ **Extintores tipo ABC** colocados estratégicamente
  - ✓ **Rutas de evacuación señalizadas**
  - ✓ **Capacitación en primeros auxilios y uso de extintores**
- Realizar **simulacros bimensuales**.

Riesgos mitigados:

- Incendios estructurales
- Pérdida de vidas o materiales
- Reacción lenta ante emergencias

Capacitación del personal en seguridad y protocolos de emergencia

Situación actual:

- No se detalla ningún plan de formación interna.

Análisis:

- El personal debe estar instruido en:
  - ✓ Reconocimiento de amenazas
  - ✓ Actuación ante incidentes de seguridad
  - ✓ Protocolo de evacuación
  - ✓ Seguridad informática básica
  - ✓ Reacción frente a extorsión o intentos de secuestro

Sugerencia:

- Incluir capacitaciones semestrales y protocolos en el manual del empleado.

Riesgos mitigados:

- Fallas humanas
- Reacciones inapropiadas en crisis
- Fuga de información

Gestión de incidentes de ciberseguridad

Situación actual:

- Uso de sistemas informáticos para inventario (potencialmente sin respaldo ni protección avanzada).

Análisis:

- Implementar una **política de seguridad informática**:
  - ✓ Antimalware y firewall activo
  - ✓ Backups diarios automáticos
  - ✓ Gestión de contraseñas y accesos por rol
  - ✓ Política de no uso de dispositivos externos sin autorización

Riesgos mitigados:

- Robo de datos
- Infección por ransomware o virus
- Pérdida de inventario por fallas o sabotaje digital

Auditorías internas para prevenir robos o pérdidas

Situación actual:

- No se especifica si se realiza un control regular de inventario o auditoría.

Análisis:

- Implementar auditorías internas mensuales:
  - ✓ Revisión de inventario físico vs. digital
  - ✓ Revisión de cámaras, accesos y reportes de incidentes
  - ✓ Control cruzado de áreas críticas (almacén, caja, sistemas)

Riesgos mitigados:

- Robo hormiga
- Mal manejo de stock
- Falsificación o manipulación de datos

Protocolo para incidentes de extorsión o secuestro

Situación actual:

- Se identificó como riesgo, pero no hay protocolos claros.

Análisis:

- Crear un **protocolo específico** para amenazas personales:
  - ✓ Contacto inmediato con autoridades locales
  - ✓ Comunicación segura y discreta
  - ✓ Plan de contención y asistencia psicológica
- Establecer un canal confidencial para reportes de amenazas.

Riesgos mitigados:

- Daños a integridad física del personal
- Ataques dirigidos a directivos
- Pánico organizacional

4.1.2. Plan estratégico en materia tecnológica

Identificación de activos y recursos críticos

Objetivo: Reconocer lo que debe ser protegido prioritariamente.

Activos identificados:

- **Personas**: empleados y directivos
- **Instalaciones**: local, puertas de acceso, almacén de productos inflamables
- **Tecnología**: computadoras, software de inventario, cámaras
- **Información**: datos personales, contables y logísticos
- **Inventario**: tableros, herrajes, insumos costosos

Acción inmediata:

- Elaborar un inventario físico y digital con niveles de criticidad.
- Etiquetar zonas y equipos de alta sensibilidad.

Detección de amenazas internas y externas

Objetivo: Identificar lo que puede causar daño o pérdida.

Amenazas externas:

- Robo/intrusión

- Incendio
- Extorsión/secuestro
- Ciberataques

Amenazas internas:

- Robo interno (empleados)
- Uso indebido de información
- Errores operativos o negligencia

Acción inmediata:

- Realizar un diagnóstico de seguridad físico y digital.
- Recolectar antecedentes de incidentes ocurridos.

Consultar con autoridades locales sobre delitos frecuentes en la zona

Tabla 18

Análisis de Vulnerabilidades

Área	Vulnerabilidad	Consecuencia Potencial	Nivel
Bodega	Material inflamable mal almacenado	Incendios, pérdida total	Alta
Sistema CCTV	Puntos ciegos o cámaras inactivas	Ingresos no detectados	Media
Puertas de ingreso	Sin refuerzo de seguridad	Fácil acceso para intrusos	Alta
Empleados	Falta de capacitación en seguridad	Fugas de información, errores humanos	Alta

Sistema informático	Ausencia de respaldo automático	Pérdida de datos, inventario	Alta
Red interna	Sin firewall ni antivirus	Ciberataques, ransomware	Alta
Gestión de claves	Accesos compartidos o débiles	Vulneración de sistemas	Alta

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Tabla 19

Matriz de Riesgos

Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Medida de Mitigación
Incendios	Alta	Alta	Crítico	Instalación de detectores de humo, extintores y capacitaciones en manejo de fuego
Robo externo	Media	Alta	Alto	Refuerzo de puertas, control de accesos, monitoreo 24/7
Robo interno	Alta	Media	Alto	Control de inventario, auditorías frecuentes, revisión de personal
Ciberataques	Alta	Alta	Crítico	Antivirus, firewall, backups regulares, contraseñas seguras
Secuestros/extorsión	Baja	Muy Alta	Alto	Protocolo de crisis, coordinación con policía, formación en seguridad personal
Falla informática	Media	Alta	Alto	Sistema de respaldo automático y mantenimiento periódico

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Diseño de estrategias y medidas de control

Objetivo: Establecer acciones para reducir o eliminar los riesgos.

Acciones clave a diseñar:

- Instalación de sensores de humo y extintores tipo ABC
- Control de accesos por tarjetas o huella
- Implementación de antivirus, firewall y backups automáticos

- Protocolos ante emergencias: fuego, intrusión, extorsión
- Capacitación al personal en manejo de crisis y seguridad informática

Acción inmediata:

- Redactar protocolos específicos por tipo de incidente.
- Crear un cronograma de implementación por prioridad.

Implementación del plan y asignación de roles

Objetivo: Ejecutar las estrategias con responsables definidos.

Roles recomendados:

- **Encargado de Seguridad Física:** supervisa accesos, cámaras, inventario.
- **Encargado de Seguridad Informática:** backups, protección de datos, antivirus.
- **Responsable de Crisis:** directivo o gerente con protocolo claro de comunicación.
- **Todo el personal:** debe participar en simulacros y capacitaciones.

Acción inmediata:

- Comunicar el plan de seguridad a todos los empleados.
- Asignar responsables por escrito y con acompañamiento.

Monitoreo, evaluación y mejora continua

Objetivo: Asegurar que las medidas funcionen y adaptarlas según sea necesario.

Tareas clave:

- Auditorías mensuales de inventario, accesos y cámaras
- Simulacros de evacuación y seguridad cada 2 meses
- Revisión de logs informáticos y respaldo mensual
- Reunión semestral de evaluación con responsables

Acción inmediata:

- Crear un calendario anual de auditorías y simulacros.
- Generar un reporte de seguridad mensual para gerencia.

4.2. Verificación de Controles

Este checklist fue utilizado para verificar distintos controles de seguridad. Para cada una de las preguntas incluidas en la tabla, se completó la siguiente información:

Respuesta: Se describió brevemente la situación observada en relación con el control evaluado.

Responsable: Se indicó el nombre de la persona que llevó a cabo la evaluación.

Fecha: Se registró la fecha en la que se realizó la evaluación correspondiente.

Tabla 20

Verificación de Controles

VERIFICACIÓN DE CONTROLES DE SEGURIDAD					
Identificador	**Aspecto a evaluar**	**Respuesta**	**Descripción**	**Responsable**	**Fecha**
ID_0001	¿La organización ha definido un documento con la política de seguridad de la información?	SI	Política aprobada por Gerencia, comunicada a todo el personal.	Área Técnica / Dirección	01/02/2024
ID_0002	¿La política de seguridad de la información se revisa periódicamente?	NO, se encuentra en desarrollo			
ID_0003	¿Se han definido las responsabilidades en materia de seguridad de la información?	SI	Roles y responsabilidades definidos en el manual de seguridad.	Dirección / Soporte TI	01/02/2024
ID_0004	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	NO			
ID_0005	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	NO formalmente			
ID_0006	¿Se dispone de un inventario de activos?	SI	Inventario digital y físico revisado semestralmente.	Área Técnica / Soporte	06/03/2018
ID_0007	¿Se ha definido quien es el responsable de los activos?	SI	Cada activo tiene un responsable	Área Técnica	06/03/2018

			asignado en el inventario.		
ID_0008	¿Se comprueban las referencias de todos los candidatos a empleo?	NO			
ID_0009	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	SI	Rejas, cámaras, recepción	Dirección Administrativa	06/03/2018
ID_0010	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	NO			
ID_0011	¿Se han definido y documentado los procedimientos operacionales TIC?	NO			
ID_0012	¿Las copias se seguridad se realizan regularmente de acuerdo con la política de backup establecida?	SI	Backups automáticos diarios en la nube.	Soporte TI	01/05/2024
ID_0013	¿Se verifica regularmente la correcta realización de las copias se seguridad?	SI	Revisión manual semanal de respaldos.	Soporte TI	22/05/2025
ID_0014	¿Se monitoriza y registra la actividad y el estado de los	NO			

	equipos críticos TIC?.				
ID_0015	¿Se registran las actividades de los administradores y operadores de sistema?	NO			
ID_0016	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?.	NO			
ID_0017	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	NO			
ID_0018	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	SI	Mediante indicaciones verbales	Soporte TI	01/02/2024
ID_0019	¿Los usuarios se aseguran de proteger los equipos desatendidos? (¿Ej. bloqueando o cerrando la sesión?	NO			
ID_0020	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	SI	Cada usuario tiene su propia cuenta de acceso.	Soporte TI	06/03/2018
ID_0021	¿Se controla la instalación de	NO			

	software en sistemas en producción?				
ID_0022	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	NO			
ID_0023	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	NO			
ID_0024	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	NO			
ID_0025	¿Se han definido, documentado e implantado planes de continuidad de negocio?	NO			
ID_0026	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	NO			
ID_0027	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	SI	Identificados y revisados anualmente por la Dirección Administrativa.	Dirección Administrativa	06/03/2018
ID_0028	¿Se han implementado procedimientos para asegurar el	SI	Procedimientos para protección de datos y cumplimiento	Dirección Administrativa	06/03/2018

	cumplimiento de los requisitos relevantes de carácter legal?		normativo implementados.
ID_0029	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	NO	
ID_0030	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	NO	

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

4.3. Inventario de Activos

Tabla 21

Inventario de activos

INVENTARIO DE ACTIVOS						
Identificador	**Nombre**	**Descripción**	**Responsable**	**Tipo**	**Ubicación**	**Crítico**
ID_0001	PC de escritorio (Recursos Humanos (RRHH))	Gestión de hojas de vida, nómina, contratos, afiliaciones	Gerente y jefe de RRHH	Servidor (físico)	Oficina administrativa	Sí
ID_0002	Laptop (Recursos Humanos (RRHH))	Gestión de hojas de vida, nómina, contratos, afiliaciones	Gerente y jefe de RRHH	Servidor (físico)	Oficina administrativa	Sí

ID_0003	PC de escritorio con software impresora (caja punto de ventas)	Facturación, gestión de ventas, cobros con tarjeta	Cajeros(as)	Servidor (físico)	Mostradores de venta	Sí
ID_0004	Impresora con acceso a (WI-FI)	Proceso de impresión mediante la red wi-fi de facturas, documentación interna y externa de la empresa, fotocopia de documentos.	Financiero	Servidor (físico)	Mostradores de venta	Sí
ID_0005	Sistema de ventas (contabilidad)	Sistema para registrar y administrar las ventas de la empresa.	Financiero / contabilidad / facturación	Servidor (aplicación)	Punto de venta	Sí
ID_0006	PC de escritorio (Atención al Cliente / Recepción)	Registro de contacto con clientes, agendamiento	Auxiliar de servicio al cliente	Servidor (físico)	Mostrador o zona de atención	Sí
ID_0007	Laptop (Atención al Cliente / Recepción)	Registro de contacto con clientes, agendamiento	Auxiliar de servicio al cliente	Servidor (físico)	Mostrador o zona de atención	Sí
ID_0008	Tablet 14 pulgadas (Bodega / Inventario)	Control de stock, entradas y salidas de producto, reportes de inventario	Auxiliar de bodega	Servidor (físico)	Área de almacenamiento	Sí

ID_0009	PC de escritorios (Bodega / Inventario)	Control de stock, entradas y salidas de producto, reportes de inventario	Encargado bodega	Servidor (físico)	Área de almacenamiento	Sí
ID_0010	Laptop (Ventas / Asesores Comerciales)	Atención a clientes, cotizaciones, seguimiento comercial	Asesores internos	Servidor (físico)	Oficinas	Sí
ID_0011	Celular corporativo (Ventas / Asesores Comerciales)	Atención a clientes, cotizaciones, seguimiento comercial	Asesores internos	Servidor (físico)	Oficinas	Sí
ID_0012	Laptop (Ventas / Asesores Comerciales)	Atención a clientes, cotizaciones, seguimiento comercial	Asesores externos	Servidor (físico)	Trabajo en campo	Sí
ID_0013	Celular corporativo (Ventas / Asesores Comerciales)	Atención a clientes, cotizaciones, seguimiento comercial	Asesores externos	Servidor (físico)	Trabajo en campo	Sí
ID_0014	Router (Red WI-FI) (Soporte técnico)	Router para la red Wifi de cortesía a los clientes.	Área técnica / soporte	Servidor (físico)	Zonas comunes	Sí
ID_0015	NVR (Network Video Recorder) (Soporte técnico)	Almacena grabaciones de cámaras IP (digitales). Se conecta a través de red	Área técnica / soporte	Servidor (físico)	Tolas las instalaciones	Sí

ID_0016	Monitor (Soporte técnico)	Pantallas para visualizar en tiempo real o grabaciones	Área técnica / soporte	Servidor (físico)	Tolas las instalaciones	Sí
ID_0017	Punto de red (soporte técnico)	Punto de red de conectividad para laptops, computadoras de escritorio e impresoras	Área técnica / soporte	Servidor (físico)	Tolas las instalaciones	Sí
ID_0018	Base de datos (Finanzas / RRHH)	Repositorio de datos con información de la empresa y clientes	Finanzas / RRH	Servidor (datos)	Oficina administrativa	Sí
ID_0019	Servidor web (página)	Base de datos, disponibles para el público	TICS	Servidor (online)	Alojamiento virtual	Si

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

4.4. Análisis de Riesgos

Tabla 22

Análisis de Riesgos

Activo	Amenaza	Probabilidad	Impacto	Riesgo
ordenador(es)	Fuga de información	Bajo (1)	Alto (3)	3
ordenador(es)	Introducción de falsa información	Bajo (1)	Alto (3)	3
ordenador(es)	Alteración de la información	Bajo (1)	Alto (3)	3
ordenador(es)	Corrupción de la información	Bajo (1)	Alto (3)	3
ordenador(es)	Destrucción de información	Bajo (1)	Alto (3)	3
ordenador(es)	Interceptación de información (escucha)	Medio (2)	Medio (2)	4

ordenador(es)	Pérdida de equipos	Medio (2)	Medio (2)	4
ordenador(es)	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
ordenador(es)	Abuso de privilegios de acceso	Medio (2)	Medio (2)	4
ordenador(es)	Acceso no autorizado	Bajo (1)	Bajo (1)	1
ordenador(es)	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
móvil(es) principalmente para telefonía	Fuga de información	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Introducción de falsa información	Medio (2)	Medio (2)	4
móvil(es) principalmente para telefonía	Alteración de la información	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Corrupción de la información	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Destrucción de información	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Interceptación de información (escucha)	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Pérdida de equipos	Medio (2)	Medio (2)	4
móvil(es) principalmente para telefonía	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
móvil(es) principalmente para telefonía	Abuso de privilegios de acceso	Bajo (1)	Medio (2)	2
móvil(es) principalmente para telefonía	Acceso no autorizado	Bajo (1)	Bajo (1)	1
móvil(es) principalmente para telefonía	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
conexión a Internet e incluso wifi	Fuga de información	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Introducción de falsa información	Bajo (1)	Bajo (1)	1
conexión a Internet e incluso wifi	Alteración de la información	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Corrupción de la información	Bajo (1)	Alto (3)	3

conexión a Internet e incluso wifi	Destrucción de información	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Interceptación de información (escucha)	Bajo (1)	Bajo (1)	1
conexión a Internet e incluso wifi	Pérdida de equipos	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Abuso de privilegios de acceso	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Acceso no autorizado	Bajo (1)	Medio (2)	2
conexión a Internet e incluso wifi	Errores del administrador	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Errores de configuración	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Denegación de servicio	Bajo (1)	Alto (3)	3
conexión a Internet e incluso wifi	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Fuga de información	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Introducción de falsa información	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Alteración de la información	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Corrupción de la información	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Destrucción de información	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Interceptación de información (escucha)	Bajo (1)	Bajo (1)	1
ordenadores y conexión a Internet (con wifi)	Pérdida de equipos	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
ordenadores y conexión a Internet (con wifi)	Abuso de privilegios de acceso	Bajo (1)	Medio (2)	2

ordenadores y conexión a Internet (con wifi)	Acceso no autorizado	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Errores del administrador	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Errores de configuración	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Denegación de servicio	Bajo (1)	Alto (3)	3
ordenadores y conexión a Internet (con wifi)	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Fuga de información	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Introducción de falsa información	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Alteración de la información	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Corrupción de la información	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Destrucción de información	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Interceptación de información (escucha)	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Pérdida de equipos	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Abuso de privilegios de acceso	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Acceso no autorizado	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Errores del administrador	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Errores de configuración	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Denegación de servicio	Bajo (1)	Alto (3)	3
dispositivos móviles para telefonía y datos	Indisponibilidad del personal	Bajo (1)	Alto (3)	3

soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Fuga de información	Bajo (1)	Alto (3)	3
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Introducción de falsa información	Bajo (1)	Alto (3)	3
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Alteración de la información	Bajo (1)	Alto (3)	3
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Corrupción de la información	Bajo (1)	Alto (3)	3
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Destrucción de información	Bajo (1)	Alto (3)	3
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso	Indisponibilidad del personal	Bajo (1)	Alto (3)	3

herramientas colaborativas o de almacenamiento cloud				
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Acceso no autorizado	Bajo (1)	Alto (3)	3
soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	Denegación de servicio	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Fuga de información	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Introducción de falsa información	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Alteración de la información	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Corrupción de la información	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Destrucción de información	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
una página web sencilla alojada y gestionada por un proveedor externo	Acceso no autorizado	Bajo (1)	Alto (3)	3

una página web sencilla alojada y gestionada por un proveedor externo	Denegación de servicio	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Fuga de información	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Introducción de falsa información	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Alteración de la información	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Corrupción de la información	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Destrucción de información	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Acceso no autorizado	Bajo (1)	Alto (3)	3
ordenadores e incluso algún servidor (web, correo electrónico,…)	Denegación de servicio	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Fuga de información	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Introducción de falsa información	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Alteración de la información	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Corrupción de la información	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Destrucción de información	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Interceptación de información (escucha)	Bajo (1)	Alto (3)	3

conexión a Internet con wifi	Pérdida de equipos	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Abuso de privilegios de acceso	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Acceso no autorizado	Bajo (1)	Alto (3)	3
conexión a Internet con wifi	Indisponibilidad del personal	Bajo (1)	Alto (3)	3
dispositivos móviles con datos y apps para su trabajo	Fuga de información	Bajo (1)	Alto (3)	3
dispositivos móviles con datos y apps para su trabajo	Introducción de falsa información	Bajo (1)	Alto (3)	3
dispositivos móviles con datos y apps para su trabajo	Alteración de la información	Bajo (1)	Alto (3)	3
dispositivos móviles con datos y apps para su trabajo	Corrupción de la información	Bajo (1)	Alto (3)	3
dispositivos móviles con datos y apps para su trabajo	Destrucción de información	Bajo (1)	Medio (2)	2
dispositivos móviles con datos y apps para su trabajo	Interceptación de información (escucha)	Bajo (1)	Medio (2)	2
dispositivos móviles con datos y apps para su trabajo	Pérdida de equipos	Bajo (1)	Medio (2)	2
dispositivos móviles con datos y apps para su trabajo	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
dispositivos móviles con datos y apps para su trabajo	Abuso de privilegios de acceso	Bajo (1)	Medio (2)	2

dispositivos móviles con datos y apps para su trabajo	Acceso no autorizado	Bajo (1)	Medio (2)	2
dispositivos móviles con datos y apps para su trabajo	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Fuga de información	Bajo (1)	Alto (3)	3
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Introducción de falsa información	Bajo (1)	Alto (3)	3
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Alteración de la información	Bajo (1)	Alto (3)	3
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Corrupción de la información	Bajo (1)	Medio (2)	2
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Destrucción de información	Bajo (1)	Alto (3)	3
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Acceso no autorizado	Bajo (1)	Medio (2)	2
herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	Denegación de servicio	Bajo (1)	Alto (3)	3
página web / tienda online y redes sociales que gestionan desde la empresa	Fuga de información	Bajo (1)	Alto (3)	3
página web / tienda online y redes sociales que gestionan desde la empresa	Introducción de falsa información	Bajo (1)	Medio (2)	2
página web / tienda online y redes sociales que gestionan desde la empresa	Alteración de la información	Bajo (1)	Alto (3)	3

página web / tienda online y redes sociales que gestionan desde la empresa	Corrupción de la información	Bajo (1)	Alto (3)	3
página web / tienda online y redes sociales que gestionan desde la empresa	Destrucción de información	Bajo (1)	Medio (2)	2
página web / tienda online y redes sociales que gestionan desde la empresa	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
página web / tienda online y redes sociales que gestionan desde la empresa	Acceso no autorizado	Bajo (1)	Medio (2)	2
página web / tienda online y redes sociales que gestionan desde la empresa	Denegación de servicio	Bajo (1)	Medio (2)	2
herramientas para empresas en la nube	Fuga de información	Bajo (1)	Alto (3)	3
herramientas para empresas en la nube	Introducción de falsa información	Bajo (1)	Medio (2)	2
herramientas para empresas en la nube	Alteración de la información	Bajo (1)	Medio (2)	2
herramientas para empresas en la nube	Corrupción de la información	Bajo (1)	Medio (2)	2
herramientas para empresas en la nube	Destrucción de información	Bajo (1)	Alto (3)	3
herramientas para empresas en la nube	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
herramientas para empresas en la nube	Acceso no autorizado	Bajo (1)	Medio (2)	2
herramientas para empresas en la nube	Denegación de servicio	Bajo (1)	Medio (2)	2
e-administración para su relación con las AAPP	Fuga de información	Bajo (1)	Medio (2)	2
e-administración para su relación con las AAPP	Introducción de falsa información	Bajo (1)	Bajo (1)	1
e-administración para su relación con las AAPP	Alteración de la información	Bajo (1)	Bajo (1)	1

e-administración para su relación con las AAPP	Corrupción de la información	Bajo (1)	Bajo (1)	1
e-administración para su relación con las AAPP	Destrucción de información	Bajo (1)	Medio (2)	2
e-administración para su relación con las AAPP	Indisponibilidad del personal	Bajo (1)	Medio (2)	2
e-administración para su relación con las AAPP	Acceso no autorizado	Bajo (1)	Medio (2)	2
e-administración para su relación con las AAPP	Denegación de servicio	Bajo (1)	Medio (2)	2

Fuente: *Elaboración propia para Multitableros & Herrajes S.A.*

4.5. Clasificación y Priorización.

Tabla 23

Clasificación y Priorización

Identificador	Título Amenaza	Descripción	Responsable	Tipo	Coste	Fecha	Revisión
IN_0001	Interceptación de información (escucha)	Implementar cifrado WPA3 en redes Wi-Fi- Uso de VPN para usuarios remotos- Contratar auditorías de red y pentesting	Área técnica / Soporte TI	Organizacional	$2500 - $5000 (posibles multas, pérdida de confianza, fuga de datos)	20/05/2025	Anual o tras incidentes
IN_0002	Pérdida de equipos	Uso de software MDM (gestión de dispositiv	Colaboradores de ventas externos / Logística / TI	operativos	$800 (reposición, recuperación de datos,	20/05/2025	Semestral

		os móviles)-Contratar seguros de equipos-Etiquetado y control de activos			riesgo de filtración)		
IN_0003	Abuso de privilegios de acceso	Separación de funciones-Auditoría de accesos-Uso de sistemas IAM (gestión de identidades y accesos)	Administradores de la empresa / TI	TI	$5000	20/05/2025	Trimestral
IN_0004	Introducción de falsa información	Capacitación periódica en calidad de datos-Controles dobles en ingreso crítico-Sistemas con validaciones automáticas	Área de ventas	Operativo	$500 - $5000	20/05/2025	Anual

Fuente: *Elaboración propia para Multitableros & Herrajes S.A.*

4.6. Check List PDS.

Tabla 24

Check List PDS

N	NIVEL	ALCANCE	CONTROL	
1	B	PRO	¿Existe una política de seguridad de la información documentada y aprobada?	☒
2	B	PRO	¿La política de seguridad se revisa periódicamente?	☒
3	B	PER	¿Se han definido y comunicado las responsabilidades en materia de seguridad?	☒
4	A	PRO	¿Existe un Comité de Seguridad encargado de la gestión de seguridad de la información?	☐
5	B	PRO	¿Los contratos con terceros incluyen cláusulas de seguridad (confidencialidad, propiedad, etc.)?	☒
6	B	TEC	¿Se dispone de un inventario actualizado de activos?	☒
7	B	PRO	¿Se ha definido el responsable de cada activo?	☒
8	B	PRO	¿Se comprueban las referencias de los candidatos a empleo?	☒
9	B	TEC	¿Existen perímetros de seguridad física (accesos controlados, cámaras, etc.)?	☒
10	A	TEC	¿Los equipos TIC críticos están ubicados en salas seguras?	☐
11	A	TEC	¿Se han documentado los procedimientos operativos TIC?	☒
12	B	TEC	¿Se realizan copias de seguridad regularmente?	☒
13	B	TEC	¿Se verifica la correcta realización de las copias de seguridad?	☒
14	A	TEC	¿Se monitoriza y registra la actividad de los equipos críticos?	☒
15	A	TEC	¿Se registran las actividades de los administradores de sistemas?	☒
16	B	TEC	¿Existe una sistemática para la asignación y uso de privilegios en los sistemas?	☒

17	B	TEC	¿Se han definido procedimientos formales para la gestión de contraseñas?	☒
18	B	PER	¿Se exige a los usuarios buenas prácticas en el uso de contraseñas?	☒
19	B	PER	¿Se protege el acceso a equipos desatendidos (bloqueo, cierre de sesión)?	☒
20	B	TEC	¿Las cuentas de usuario son unipersonales?	☒
21	B	TEC	¿Se controla la instalación de software en sistemas en producción?	☒
22	A	TEC	¿Existe un proceso para la gestión de vulnerabilidades técnicas?	☒
23	A	PRO	¿Se ha documentado un proceso para la gestión de incidentes de seguridad?	☒
24	A	PRO	¿Existe un plan de continuidad de negocio documentado?	☒
25	A	PRO	¿Se revisan y prueban los planes de continuidad de negocio?	☐
26	B	PRO	¿Se identifican y cumplen los requisitos legales relevantes?	☒
27	B	PRO	¿Existen procedimientos para asegurar el cumplimiento de requisitos legales?	☒
28	A	PRO	¿Se han establecido procedimientos para la protección y privacidad de la información?	☒
29	A	TEC	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a estándares?	☐

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Análisis de Cambios

Mejoras significativas:

- Se implementaron controles clave como revisión de la política de seguridad, inclusión de cláusulas en contratos, documentación de procedimientos TIC, gestión de incidentes y vulnerabilidades.
- Se avanzó en la protección de la información y la formalización de procesos de RRHH.

Pendientes o parciales:

- La creación del Comité de Seguridad sigue pendiente.
- La ubicación física segura de equipos TIC críticos requiere inversión.
- Las pruebas y revisiones periódicas de continuidad de negocio y adecuación a estándares necesitan consolidarse como prácticas regulares.

Controles sin cambio:

- Algunos controles básicos ya estaban implementados y se mantienen, como la existencia de políticas, inventarios, y cumplimiento legal.

CAPITULO 5

PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN BASADO EN LA NORMA ISO 31000:2028

Empresa: Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.

Ubicación: Quevedo, Ecuador.

5. DESARROLLO DEL CONTENIDO

5.1. Objeto y campo de aplicación

Esta propuesta tiene como objetivo implementar un Sistema de Gestión de Riesgos en la empresa Megamaderas & Herrajes – Sucursal Quevedo, de acuerdo con los lineamientos establecidos en la norma ISO 31000:2018. La finalidad es mejorar la toma de decisiones, aumentar la eficiencia operativa y garantizar la continuidad del negocio frente a riesgos internos y externos.

El campo de aplicación comprende todas las áreas operativas y administrativas de la sucursal, incluyendo:

- Recepción y despacho de materiales: Se controla la entrada y salida de los productos, como también la verificación de calidad y cantidad de los pedidos.
- Inventario y almacenamiento: Se gestiona y se controla la organización física de los productos del inventario en el local.
- Atención al cliente: Se realiza la asesoría y cotizaciones de los productos a los clientes.

- Seguridad física: Se debe contemplar la protección de empleados, activos y de las instalaciones, en caso de riesgos o problemáticas que puedan afectar al entorno.
- Recursos humanos: Se realizan gestiones específicas como la contratación y capacitación del personal.
- Cumplimiento normativo: Se realizan seguimientos laborales, ambientales y tributarios.

Análisis FODA

Tabla 25

Análisis FODA – Megamaderas & Herrajes (Sucursal Quevedo)

Fortalezas	**Oportunidades**
- Personal con experiencia en atención al cliente y manejo de inventario.	- Aumento en la demanda de productos de madera por el sector de construcción.
- Reputación local consolidada.	- Posible expansión digital (ventas online).
- Buena ubicación geográfica (fácil acceso para clientes y proveedores).	- Alianzas estratégicas con carpinterías y constructoras.
- Variedad de productos en stock.	- Acceso a programas de capacitación empresarial o subsidios gubernamentales.
Debilidades	**Amenazas**
- Ausencia de un sistema formal de gestión de riesgos.	- Inseguridad ciudadana (robos, asaltos).

- Dependencia de un número reducido de proveedores clave.	- Competencia de grandes cadenas de ferreterías.
- Bajo nivel de digitalización (ventas y control de stock manual o semiautomatizado).	- Variaciones de precios en materia prima.
- Falta de capacitación constante del personal en temas de ciberseguridad y prevención de riesgos.	- Fallas en servicios públicos (eléctricos o de conectividad).

Fuente: *Elaboración propia para Multitableros & Herrajes S.A.*

5.2. Referencias Normativas

Aunque la **ISO 31000:2018** no contiene normas obligatorias complementarias, se recomienda considerar las siguientes para reforzar el sistema de gestión de riesgos:

- ISO/IEC 31010:2019: Técnicas de evaluación de riesgos
- ISO 9001:2015: Gestión de la calidad
- ISO 45001:2018: Seguridad y salud en el trabajo (relevante por las condiciones físicas del personal)
- Constitución de la República del Ecuador.
- Código del Trabajo.
- Ley Orgánica de Salud y Seguridad del Trabajo.
- Normas del Instituto Ecuatoriano de Seguridad Social (IESS).
- Código Orgánico Integral Penal (COIP) – en lo relativo a delitos por omisión de gestión de riesgos.

- Ley Orgánica de Seguridad Integral (Ecuador).
- Código de Trabajo del Ecuador (aspectos de seguridad laboral).
- Reglamento de Seguridad contra Incendios y Emergencias (Ministerio del Interior, Ecuador).
- Normas técnicas locales para sistemas de videovigilancia y protección de datos personales.
- Ley Orgánica de Seguridad Pública y del Estado (Relacionada con la gestión de riesgos y emergencias a nivel nacional).
- Ley Orgánica de Protección de Datos Personales (LOPDP) (Fundamental si la empresa usa videovigilancia o maneja datos de empleados y clientes).
- Reglamento de Seguridad y Salud de los Trabajadores y Mejoramiento del Medio Ambiente de Trabajo (Emitido por el Ministerio de Trabajo; contiene obligaciones específicas de prevención)
- Norma Técnica INEN 0045: Gestión de la seguridad y salud en el trabajo (Norma ecuatoriana que complementa la ISO 45001).
- Ordenanzas municipales específicas de Quevedo relacionadas con la seguridad ocupacional y comercial (Pueden incluir requisitos para licencias, horarios, señalización, extintores, etc.).

5.3. Términos y definiciones

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Contexto: Entorno interno y externo en el que opera la organización.

Parte interesada: Persona u organización que puede afectar o ser afectada por una decisión o actividad.

Evaluación del riesgo: Proceso general de identificación, análisis y evaluación.

Tratamiento del riesgo: Selección e implementación de medidas para modificar el riesgo.

Incidente: Evento no deseado que puede afectar la seguridad, operación o integridad.

Criterios de riesgo: Términos de referencia contra los cuales se mide la significancia del riesgo. Se basan en objetivos, requisitos legales y otros factores contextuales.

Mapa de riesgos: Representación visual de los riesgos identificados, clasificados por su probabilidad e impacto.

Vulnerabilidad: Debilidad interna que puede ser explotada por amenazas y aumentar la probabilidad o impacto de un riesgo.

Probabilidad: Posibilidad de que ocurra un evento específico en un tiempo determinado.

Consecuencia: Resultado o impacto de un evento que afecta los objetivos organizacionales.

Monitoreo: Observación sistemática y continua del riesgo y del sistema de gestión, para detectar cambios o desviaciones.

Revisión: Evaluación programada del sistema de gestión para determinar su eficacia y oportunidades de mejora.

5.4. Principios de Gestión del Riesgo

La implementación en Megamaderas & Herrajes se regirá por los 8 principios establecidos en la norma:

5.4.1. Integrada

La gestión del riesgo estará integrada en todos los procesos clave de la empresa:

- Control de inventario
- Manejo de caja
- Seguridad física del local y activos
- Evaluación de proveedores
- Seguridad laboral y salud ocupacional

5.4.2. Estructuradas y exhaustiva

Se aplicará un enfoque sistemático, con un mapa de riesgos por área (ventas, bodega, atención al cliente, seguridad, compras), asegurando cobertura total de procesos y actores. Se utilizarán herramientas como matrices de riesgo, análisis FODA y auditorías internas para asegurar una cobertura total.

5.4.3. Adaptada

El sistema se adapta a la realidad de la sucursal, su tamaño (26 empleados), y características específicas como el manejo de MDF y ferretería, así como la infraestructura tecnológica y de vigilancia:

- Riesgos primarios: robo, pérdida de inventario, accidentes laborales, problemas logísticos.
- Evaluación mensual, reporte al Gerente General.

5.4.4. Inclusiva

La participación de todas las partes interesadas es esencial, incluyendo a empleados, proveedores, clientes y autoridades locales, para asegurar que todos los puntos de vista sean considerados y para promover una cultura de prevención y la retroalimentación sobre riesgos identificados en sus funciones diarias:

- Encuestas internas trimestrales
- Buzón de sugerencias
- Charlas de sensibilización
- Comité interno de riesgos con representación de cada área

5.4.5. Dinámica

El sistema será sensible a cambios para adaptarse a cambios externos e internos:

- Actualización del análisis de riesgo cada 6 meses
- Inclusión de nuevos proveedores, cambios en inventario, cambios en legislación o incidentes de seguridad, rotación de personal
- Monitoreo en tiempo real con apoyo de cámaras y reporte del supervisor de turno

5.4.6. Mejor información disponible

Se tomarán decisiones basadas en datos reales y actualizados, como:

- Datos históricos (robos, accidentes, devoluciones)
- Reportes de proveedores
- Informes de supervisores

- Normativa legal vigente
- Análisis de entorno comercial de Quevedo
- Resultados de auditorías internas

5.4.7. Factores humanos y culturales

La cultura de seguridad y prevención será promovida a través de capacitaciones periódicas, reforzando la responsabilidad individual y colectiva, respeto a la cultura organizacional y política de cero tolerancias al acoso, sobornos o fraude.

5.4.8. Mejora continua

Se establecerán ciclos de revisión, evaluación y mejora del sistema, a través de auditorías internas, reuniones de seguimiento y actualizaciones del plan de riesgos.

5.5. Marco de referencia

5.5.1. Generalidades

La gestión de riesgos tiene como propósito constante crear y resguardar el valor dentro de la organización, en este contexto Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. ha daptado la norma ISO 31000:2018 como base para el diseño e implementación de su sistema de Gestion de riesgos, con el objetivo de proteger su valor organizacional y asegurar el cumplimiento de sus metas estratégicas y opetaivas. Esta decicion busca mejorar el desempeño institucional, impulsar la innovación y fortalecer el compromiso de sus colaboradores.

Los principios expuestos en la Mision, visión y valores, de este documento ofrecen una guía Clara sobre las características esenciales de una gestión de riesgos eficaz eficiente destacando su propósito valor e intención dichos principios son Pilares fundamentales para establecer tanto el marco de referencia como los procesos de sistemas de gestión De riesgos de la empresa y permiten enfrentar adecuadamente los efectos de la incertidumbre en la relación con los objetivos trazados.

5.5.2. Liderazgo y compromiso

A continuación, se representa las políticas de gestión de riesgos de Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.

- La gestión de riesgos en Multitableros & Herrajes, S.A. está alineada con sus objetivos estratégicos la empresa ha asumido el compromiso de implementar un sistema de gestión de riesgos que funcione como una herramienta de apoyo para alcanzar sus metas y conservar el valor actual al mismo tiempo que impulsa la generación de valor a futuro.
- Esta gestión tiene un enfoque integral facilitando la identificación análisis evaluación y tratamiento de los riesgos a los que está expuesto la organización.
- La iniciativa para la gestión de riesgos surge desde la alta dirección y se dispone a todos los niveles promoviendo una cultura organizacional centrada en la gestión basada en riesgos.
- El sistema abarca todos los procesos que conforman la cadena de valor de la empresa.
- El seguimiento y cumplimiento de sistema de gestión de riesgos está a cargo del comité de riesgos que se conformara según el planeamiento de estrategias internas de la organización.

- La alta dirección tiene la responsabilidad de asegurar la disponibilidad de los recursos necesarios para una gestión eficaz de riesgos.
- La empresa se compromete a realizar una valoración de riesgos al menos una vez al año o cuando se presenten cambios significativos de sus objetivos o factores externos que pueden impactar sus operaciones.
- El sistema será actualizado de manera continua como parte de un proceso de mejora permanente que permita detectar oportunidades de optimismo de optimización y retroalimentación del mismo.
- Todos los colaboradores tienen el deber de reportar cualquier evento que represente un riesgo a la organización.

5.5.3. Integración

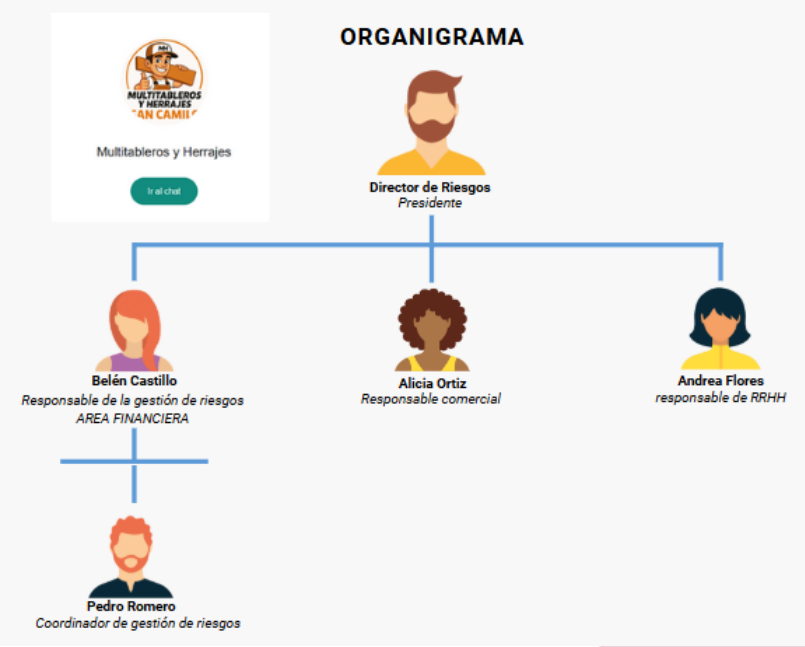
Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. ha decidido fortalecer su sistema organizacional mediante la integración de la gestión de riesgos a todos los procesos clave que conforman su cadena de valor esta edición responde a una visión estratégica de la alta dirección que reconoce en la gestión de riesgos una herramienta esencial para incrementar el valor de la organización y fortalecer la confianza de sus partes interesadas con este enfoque se establece que el sistema de gestión de riesgos abarcará el mismo alcance que los procesos operativos y estratégicos actuales incluyendo desde la planificación hasta la ejecución de proyectos y actividades cotidianas la integración de este sistema permitirá anticipar y gestionar de manera proactiva los posibles

eventos que puedan afectar el cumplimiento de los objetivos institucionales para lograr una implementación efectiva se contempla:

- La incorporación de la gestión de riesgos en todos los niveles de la organización asegurando que conforme parte tanto de la planificación estratégica como de las operaciones diarias y la gestión de proyectos.
- la capacitación continua del personal orientada a que cada colaborador comprenda su rol dentro del sistema de gestión de riesgos, así como el impacto que sus actividades pueden tener en la exposición al riesgo y en la residencia organizacional la supervisión de este sistema estará a cargo del comité de riesgos el cual será conformado de la siguiente manera:

Figura 12

Organigrama



Fuente: Organigrama Estructural Detallado Fuente: Multitableros & Herrajes, S.A. (2025)

Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. conformara el comité de riesgos por un equipo de colaboradores responsables de liderar coordinar y fortalecer la gestión de riesgos dentro de la empresa entre sus principales funciones destacan.

- promover y difundir la política de gestión de riesgos en todos los niveles de la organización asegurando su comprensión y correcta aplicación por parte de todos los colaboradores.
- Designar un vocero y definir el canal de comunicación oficial con las partes interesadas en caso de que se materialice un evento de riesgos que afecten a la empresa o su entorno.
- Evaluar y validar la metodología utilizada para la identificación análisis y tratamiento y monitoreo de los riesgos dentro de la organización.
- Establecer el apetito de riesgo de la empresa es decir el nivel de riesgo que la empresa. Multitableros & Herrajes, S.A., está dispuesta a asumir para alcanzar sus objetivos estratégicos.
- Identificar posibles escenarios de riesgos que puedan comprometer el logro de los objetivos institucionales o poner en peligro la continuidad del negocio.
- Evaluar la efectividad del sistema de gestión de riesgos verificando el desempeño de los controles implementados y supervisando su cumplimiento por parte de los respectivos responsables de la gestión de riesgos.

- Fomentar una cultura organizacional basada en la gestión de riesgos promoviendo la conciencia participación activa y responsabilidad de todos los miembros de la empresa frente a los riesgos que pueden surgir.

5.5.4. Diseño

Nuestro diseño del marco de referencia considera el contexto de la organización, su misión, visión, valores, estructura, recursos, partes interesadas y entorno externo e interno.

Misión

La empresa Multitableros & Herrajes S.A. tiene como misión proporcionar a sus clientes productos ferreteros con altos estándares de calidad, con un servicio eficiente y precios módicos. La empresa busca satisfacer las necesidades de sus consumidores mediante una atención personalizada y especializada, con una oferta que combine disponibilidad, variedad y responsabilidad comercial.

Visión

La empresa Multitableros & Herrajes S.A. busca consolidarse como una de las principales ferreterías a nivel país, destacando por su capacidad de ofrecer productos de alta calidad y un servicio técnico especializado. Su visión a mediano plazo es ser reconocida por su responsabilidad con los clientes, la atención personalizada y la mejora continua, aportando al crecimiento del sector ferretero.

Valores

Responsabilidad: Cumplir con los compromisos de trabajo con clientes, colaboradores y proveedores, de manera ética y oportuna.

Compromiso con el cliente: Brindar una atención de calidad, eficaz y honesta, enfocada en resolver las necesidades reales de cada proyecto.

Seguridad: Priorizar la seguridad de los trabajadores y clientes, promoviendo prácticas que prevengan riesgos e incentivando a la seguridad empresarial.

5.5.4.1. Comprensión de la organización y su contacto

La empresa es una ferretería con 14 años de experiencia, dedicada a la venta mayorista y minorista de materiales de construcción, herrajes, madera, y otros productos afines, con operaciones en Quevedo y la provincia de Los Ríos. Sus principales riesgos están asociados a la continuidad operativa, seguridad de la información, cumplimiento legal, salud ocupacional, reputación y riesgos tecnológicos/cibernéticos. Factores relevantes del contexto:

- Entorno competitivo local y nacional.
- Dependencia de proveedores internacionales.
- Regulaciones nacionales sobre protección de datos y seguridad industrial.
- Cultura organizacional basada en la responsabilidad, integridad y trabajo en equipo.

Tabla 26

ANÁLISIS PESTEL - Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.

FACTOR	DESCRIPCIÓN
Político	• **Estabilidad política en Ecuador**: Influye en la confianza de consumidores y empresas. • **Regulaciones municipales y nacionales**: Licencias, permisos de funcionamiento, patentes, horarios comerciales. • **Importaciones y comercio exterior**: Reglas aduaneras, grabación de IVA, aranceles y tratados comerciales afectan los costos y disponibilidad de productos. • **Iniciativas públicas de construcción**: Inversión en proyecto de infraestructura y vivienda impulsan la demanda.
Económico	• **Inflación y tipo de cambio**: Impacto directo en los precios de productos importados y márgenes de ganancia. • **Crecimiento del sector construcción**: Motor primordial para la demanda de materiales ferreteros. • **Acceso a financiamiento**: Necesidad de capital para expansión, innovación y gestión de riesgos. • **Poder adquisitivo**: Cambios en el ingreso y falta de circulante económico de los clientes afectan la frecuencia y volumen de compra.

	• **Competencia de precios**: Presión por parte de grandes cadenas y plataformas digitales, crean monopolios que afectan al consumo.
Social	• **Tendencia de mano de obra no calificada profesionalmente y mejoras del hogar**: Creciente interés en hacer reparaciones y mejoras por cuenta propia. • **Demografía local**: Zonas urbanas en expansión, nuevos proyectos habitacionales. • **Valoración del servicio personalizado**: Los clientes buscan asesoría con empresas de confianza, lo que favorece a negocios con atención directa. • **Preferencia por productos ecológicos**: Demanda de pinturas sin tóxicos, materiales reciclados, soluciones eficientes.
Tecnológico	• **Digitalización y comercio electrónico**: Crecimiento en la venta online y uso de sistemas de gestión avanzados que facilita al cliente la compra. • **Innovación en productos**: Nuevas herramientas, materiales y soluciones tecnológicas para construcción y hogar. • **Seguridad de la información**: Necesidad de fortalecer la protección de datos y sistemas frente a ciber amenazas. • **Automatización y gestión de inventario**: Uso de software para mejorar eficiencia y control.
Ecológico	• **Normativas ambientales**: Restricciones sobre productos contaminantes, gestión de residuos y reciclaje.

	• **Tendencia hacia la sostenibilidad**: Oportunidad para diferenciarse con productos ecológicos y procesos responsables. • **Eventos climáticos extremos**: Riesgo de afectaciones logísticas y de inventario.
Legal	• **Leyes de protección de datos personales**: Obligación de cumplir con la LOPDP y normativas de privacidad. • **Normativas laborales**: Seguridad y salud ocupacional, equidad de género, contratos y derechos laborales. • **Regulación de productos**: Cumplimiento de estándares de calidad, seguridad y etiquetado. • **Propiedad intelectual**: Respeto a marcas, patentes y derechos de autor en productos y servicios.

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

5.5.4.2. Articulación del compromiso con la gestión del riesgo

El compromiso de la alta dirección debe formalizarse a través de:

- Una política de gestión de riesgos aprobada y difundida.
- Inclusión de la gestión de riesgos en los objetivos estratégicos.
- Integración de la gestión de riesgos en los planes operativos y de mejora continua.
- Participación activa en la revisión y seguimiento de los procesos de gestión de riesgos.

En base a lo anterior mencionado, la organización establece el siguiente compromiso:

Política de Gestión de Riesgos

Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.

1. Propósito

La presente política establece el compromiso de Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. con la gestión proactiva, sistemática y transversal de los riesgos que puedan afectar el logro de nuestros objetivos estratégicos, operativos, financieros, legales, tecnológicos, ambientales y reputacionales.

El propósito es fortalecer la resiliencia organizacional, proteger a nuestros colaboradores, clientes y partes interesadas, y asegurar la sostenibilidad y competitividad de la empresa.

2. Importancia de la gestión de riesgos

La gestión de riesgos es un componente esencial en todos los procesos y decisiones de la organización. Permite anticipar, identificar, evaluar, tratar, monitorear y comunicar los riesgos, minimizando impactos negativos y aprovechando oportunidades para el crecimiento y la mejora continua.

Una adecuada gestión de riesgos contribuye al cumplimiento normativo, la protección de los activos, la confianza de clientes y proveedores, y la creación de valor para los accionistas y la sociedad.

3. Alcance

Esta política es de aplicación obligatoria para todos los empleados, directivos, socios, proveedores y colaboradores de la empresa, sin distinción de nivel jerárquico o área funcional.

Incluye tanto los riesgos internos como externos, y abarca los procesos operativos, comerciales, administrativos, tecnológicos y estratégicos.

4. Principios de la gestión de riesgos

La gestión de riesgos en Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. se basa en los siguientes principios:

- **Integración**: La gestión de riesgos está integrada en todos los procesos y decisiones de la organización.
- **Proactividad y anticipación**: Se promueve la identificación temprana y el tratamiento oportuno de los riesgos.
- **Participación y responsabilidad**: Todos los niveles y áreas son responsables de identificar y gestionar los riesgos en su ámbito de acción.
- **Transparencia y comunicación**: Se fomenta la comunicación clara y oportuna de los riesgos y sus tratamientos.
- **Mejora continua**: Los procesos de gestión de riesgos se revisan y mejoran periódicamente para adaptarse a los cambios internos y del entorno.
- **Cumplimiento normativo**: Se asegura el cumplimiento de la legislación vigente y las mejores prácticas internacionales (ISO 31000).

5. Compromisos de la organización

- Proveer los recursos necesarios (humanos, tecnológicos y financieros) para una gestión efectiva de los riesgos.
- Capacitar y sensibilizar a todo el personal sobre la importancia y las prácticas de gestión de riesgos.
- Definir roles, responsabilidades y autoridades claras para la gestión de riesgos.
- Establecer mecanismos de reporte, monitoreo y revisión de los riesgos y sus controles.
- Promover una cultura organizacional orientada a la prevención, resiliencia y mejora continua.

6. Responsabilidades

- **Alta Dirección**: Liderar el compromiso, aprobar la política y supervisar su cumplimiento.
- **Gerencias y Jefaturas**: Implementar la política en sus áreas, identificar y reportar riesgos, y ejecutar los planes de tratamiento.
- **Empleados y colaboradores**: Participar activamente en la identificación y gestión de riesgos, reportar incidentes y sugerir mejoras.

7. Revisión y actualización

La presente política será revisada al menos una vez al año, o cuando ocurran cambios significativos en la organización o su entorno, para asegurar su vigencia y efectividad.

Aprobado por:

Gerente General

Fecha: 12/06/2025

Versión: 1.0

5.5.4.3. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización

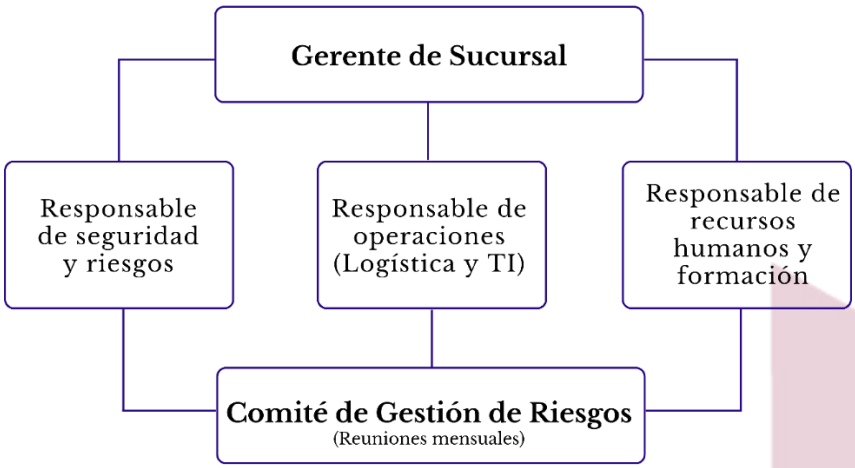
Objetivo General:

Establecer una estructura clara que permita identificar, evaluar, tratar, monitorear y comunicar los riesgos dentro de la sucursal, integrando esta función con las operaciones diarias.

- El Gerente General es el responsable último de la gestión de riesgos.
- Cada jefe de departamento (operaciones, ventas, administración, marketing, finanzas) es responsable de la gestión de riesgos en su área.
- Se designará un Comité de Gestión de Riesgos, integrado por miembros de las principales áreas, que coordinará las actividades, revisará incidentes y propondrá mejoras.
- Todos los empleados deben participar activamente en la identificación y reporte de riesgos.

Figura 13

Organigrama estructural propuesto



Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Roles y Responsabilidades

Gerente de Sucursal

- Aprobar políticas y planes de gestión de riesgos.
- Garantizar los recursos necesarios para el control y prevención.
- Liderar la toma de decisiones estratégicas ante riesgos críticos.

Responsable de Seguridad y Riesgos

- Coordina el Sistema de Gestión de Riesgos.
- Lleva el registro y evaluación de riesgos.
- Elabora informes de riesgo para la gerencia.
- Coordina acciones con los otros responsables funcionales.

Responsable de Operaciones (Logística y TI)

- Identifica y reporta riesgos operativos y tecnológicos.
- Garantiza la seguridad física de la mercancía.
- Implementa medidas de protección de datos y redes.

Responsable de RR.HH. y Formación

- Promueve la cultura de prevención de riesgos.
- Planifica y ejecuta capacitaciones en seguridad física y digital.
- Administra el plan de respuesta ante emergencias (incluye salud y seguridad laboral).

Comité de Gestión de Riesgos

- Integrado por los responsables mencionados y liderado por el Gerente.
- Se reúne de forma mensual o en caso de incidentes relevantes.
- Evalúa nuevos riesgos, seguimiento de incidentes y propone mejoras continuas.

Ventajas de esta estructura

- Es horizontal y práctica, adecuada para el tamaño de la sucursal.
- Promueve la colaboración entre áreas.
- Facilita la toma de decisiones rápidas y seguimiento efectivo.
- No requiere contratar nuevo personal, se basa en asignar roles dentro de los actuales cargos.

5.5.4.4. Asignación de recursos

Para implementar y mantener el marco de gestión de riesgos, la organización debe contar con:

Tabla 27

Identificación y provisión de recursos necesarios

Tipo de recurso	Detalle y propósito	Estado actual	Propuesta / Acción
Recursos humanos	Personal para liderar y coordinar la gestión de riesgos (comité de riesgos, responsables por área).	Parcialmente cubierto	Designar responsables por área y crear un Comité de Gestión de Riesgos.
Capacitación	Formación en gestión de riesgos, ISO 31000, seguridad de la información, manejo de incidentes.	Limitada	Implementar un plan anual de capacitación para todo el personal.
Tecnología	Sistemas de gestión de riesgos, software de inventario, seguridad informática (antivirus, firewall, backups).	Básica	Adquirir o actualizar software especializado y reforzar la ciberseguridad.
Herramientas	Manuales, procedimientos,	Parcial	Desarrollar y distribuir manuales y formatos

	formatos para identificación, análisis y reporte de riesgos.		actualizados.
Presupuesto	Recursos financieros para capacitación, adquisición de tecnología, consultoría y mejora continua.	Limitado	Asignar un presupuesto específico anual para gestión de riesgos y su mejora continua.
Consultoría externa	Asesoría para implementación, auditoría y mejora del sistema de gestión de riesgos.	No disponible	Contratar consultores especializados para acompañar la implementación y auditoría periódica.

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Capacitación y presupuesto

- **Capacitación:**
    - Realizar talleres y cursos sobre gestión de riesgos, seguridad de la información y respuesta a incidentes.
    - Incluir simulacros y ejercicios prácticos.

- Capacitar a todo el personal, con énfasis en mandos medios y responsables de procesos críticos.

- **Presupuesto:**
  - Definir una partida presupuestaria anual para:
    - Cursos y talleres.
    - Licencias de software.
    - Consultoría y auditoría.
    - Mejoras en infraestructura tecnológica y física.

5.5.4.5. Establecimiento de la comunicación y la consulta

Tabla 28

Plan de comunicación interna y externa

Audiencia	Mensaje principal	Medio / Herramienta	Frecuencia
Empleados	Objetivos, avances y responsabilidades en gestión de riesgos	Reuniones, emails, carteleras	Mensual/Trimestral
Alta dirección	Resultados, auditorías, incidentes relevantes	Reportes ejecutivos, reuniones	Trimestral
Proveedores	Requisitos de seguridad, buenas prácticas	Emails, contratos, reuniones	Anual
Clientes	Compromiso con la seguridad, manejo de incidentes	Web, redes sociales, comunicados	Según necesidad
Comunidad y reguladores	Cumplimiento normativo, transparencia	Reportes, sitio web, eventos	Anual

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Consulta regular con partes interesadas

- **Encuestas y entrevistas** periódicas a empleados sobre percepción y cultura de riesgos.
- **Reuniones de retroalimentación** con proveedores y clientes clave.
- **Buzón de sugerencias** y canal anónimo para reportar riesgos o incidentes.
- **Participación en foros sectoriales** para conocer tendencias y expectativas externas.

5.5.5. Implementación

Pasos clave para la implementación del marco de gestión de riesgos:

1. **Aprobación y difusión de la política de gestión de riesgos** a todos los niveles de la organización.
2. **Conformación del Comité de Gestión de Riesgos** y designación de responsables por área.
3. **Capacitación inicial** a todo el personal.
4. **Desarrollo y distribución de manuales y procedimientos** para identificación, análisis, tratamiento y reporte de riesgos.
5. **Implementación de herramientas tecnológicas** (software de gestión, sistemas de seguridad).
6. **Integración de la gestión de riesgos en los procesos operativos y estratégicos** (ventas, compras, logística, atención al cliente, etc.).
7. **Comunicación continua** de avances, incidentes y buenas prácticas.

8. **Seguimiento y registro** de riesgos, controles y acciones correctivas.

5.5.6. Valoración

Valoración de riesgos

- **Identificación de riesgos:** Mapear todos los riesgos relevantes en procesos, activos, personas y entorno.
- **Análisis y evaluación:**
  - Determinar probabilidad e impacto de cada riesgo.
  - Utilizar matrices de riesgo y criterios definidos (por ejemplo, bajo/medio/alto).
- **Priorización:**
  - Focalizar recursos en los riesgos con mayor impacto/probabilidad.
  - Documentar riesgos críticos y planes de acción asociados.

Herramientas recomendadas:

- Matriz de riesgos (Impacto vs Probabilidad).
- Registro de riesgos.
- Indicadores clave de riesgos (KRIs).
  - Medir periódicamente la eficacia del sistema de gestión de riesgos mediante auditorías internas, revisiones de indicadores y análisis de incidentes.
  - Evaluar el cumplimiento de los objetivos y la adecuación de los controles implementados.
  - Recoger retroalimentación de empleados y partes interesadas para identificar áreas de mejora.

5.5.7. Mejora

5.5.7.1. Adaptación

Adaptación y mejora continua

- **Revisión periódica** del marco de gestión de riesgos (al menos una vez al año o tras incidentes relevantes).
- **Actualización de políticas y procedimientos** según cambios en el entorno, la normativa o la organización.
- **Capacitación continua** y actualización de conocimientos al personal.
- **Retroalimentación y lecciones aprendidas** tras incidentes, auditorías o simulacros.
- **Innovación en herramientas y tecnologías** para responder a nuevas amenazas (ciberseguridad, protección de datos, etc.).

5.5.7.2. Mejora continua

La mejora continua es importante para cumplir con la eficacia del sistema, siempre y cuando se cumplan con lo siguiente:

Revisión periódica del proceso de gestión de riesgos.

Lecciones aprendidas de eventos anteriores o cambios del entorno.

Auditorías internas y externas.

Retroalimentación de todos los actores del proceso.

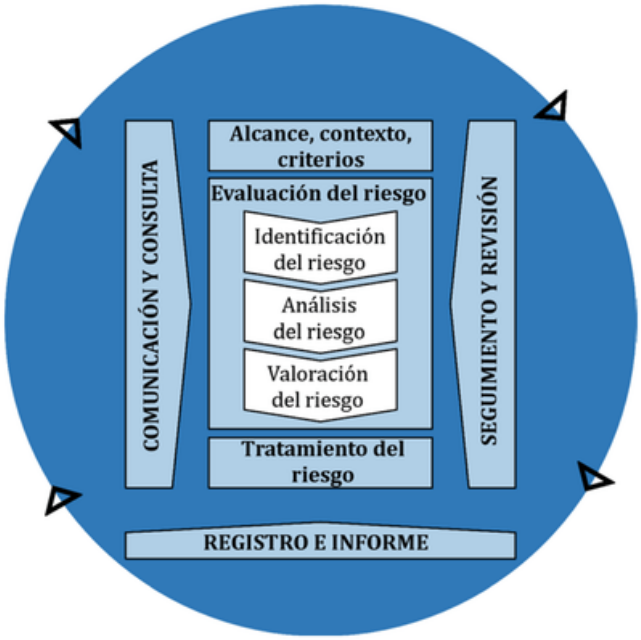
La organización debe establecer mecanismos claros capaces de identificar oportunidades propendiendo a la mejora continua y actualización de políticas, procedimientos y metodologías conforme sea necesario. Con este enfoque se asegura que el sistema siga siendo relevante, eficaz y alineado con los objetivos empresariales.

- Fomentar la cultura de mejora continua en la gestión de riesgos.
- Actualizar políticas, procedimientos y controles de acuerdo con las mejores prácticas y la evolución de los riesgos.
- Promover la innovación y la participación de todo el personal en la identificación de oportunidades de mejora.

5.6. Proceso

Figura 14

Proceso de la Gestión del Riesgo ISO 31000



***Fuente**: ISO.org*

5.6.1. Generalidades

La implementación de un proceso de gestión de riesgos tiene como objetivo identificar, analizar, evaluar, tratar, monitorear y revisar los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos y operativos de Ferretería Multitableros & Herrajes S.A. ubicada en la ciudad de Quevedo. Este proceso será sistemático, estructurado, oportuno y basado en la mejor información disponible, fomentando una cultura de gestión del riesgo en todos los niveles. Este proceso proporciona una base estructurada para:

- Tomar decisiones informadas.
- Reducir la incertidumbre.
- Proteger los activos de la organización.
- Aumentar la eficiencia operativa.
- Asegurar el cumplimiento de objetivos estratégicos.

Este enfoque será continuo, adaptativo y alineado con el contexto y necesidades específicas de la empresa.

5.6.2. Comunicación y consulta

Objetivo:

Garantizar que todos los trabajadores comprendan los riesgos relacionados a sus actividades, participen en su gestión y control.

Acciones prácticas:

- Reuniones mensuales de 30 min por área para identificar incidentes o riesgos.
- Cuadro informativo en la sala de empleados con “Riesgos del mes” y “Recomendaciones”.
- Buzón físico y/o digital para que los trabajadores reporten riesgos de manera voluntaria.
- Designar a un **"responsable de riesgos" por área** (jefe de bodega, jefe de caja, encargado de entregas)

Acciones propuestas:

- Establecer un **Plan de Comunicación de Riesgos** interno y externo.
- Crear un **Comité de Gestión de Riesgos** multidisciplinario.
- Implementar canales formales de consulta (correo, buzones, formularios digitales).
- Capacitar al personal sobre identificación y reporte de riesgos.

Herramientas sugeridas:

- Mapas de stakeholders.
- Reuniones participativas (focus group).
- Encuestas de percepción de riesgos.
- Boletines informativos

5.6.3. Alcance, contexto y criterios

5.6.3.1. Generalidades

Para una implementación efectiva, es necesario establecer claramente el alcance, comprender el contexto interno y externo, y definir los criterios de evaluación de riesgos. Esto permite adaptar el sistema a las características únicas de la organización.

5.6.3.2. Definición del alcance

1. Procesos, actividades y decisiones objeto de gestión de riesgos

El sistema de gestión de riesgos abarcará los siguientes procesos, actividades y decisiones dentro de la organización:

Procesos Operativos

- **Recepción y almacenamiento de inventarios:** Control de calidad, manejo y almacenamiento seguro de productos, prevención de pérdidas, robos y deterioro.
- **Venta y atención al cliente:** Proceso de facturación, manejo de efectivo, uso de terminales electrónicas, asesoría técnica, atención en tienda física y canales digitales.
- **Entrega y despacho de productos:** Logística de entrega a domicilio, transporte, control de pedidos y devoluciones.
- **Corte y personalización de materiales:** Manejo de maquinaria, seguridad industrial, calidad del producto final.

Procesos Administrativos y Financieros

- **Gestión de compras y proveedores:** Selección, negociación y evaluación de proveedores, importación de insumos, gestión de pagos.
- **Gestión de recursos humanos:** Contratación, capacitación, seguridad y salud ocupacional, manejo de nómina y clima laboral.
- **Gestión financiera y contable:** Control de ingresos y egresos, cumplimiento tributario, administración de cuentas bancarias.

Procesos Comerciales y de Marketing

- **Estrategias de ventas y promociones:** Decisiones sobre precios, descuentos, campañas publicitarias.
- **Gestión de clientes y relaciones públicas:** Manejo de reclamos, fidelización y satisfacción del cliente.
- **Gestión de canales digitales:** Comercio electrónico, redes sociales, protección de datos personales de clientes.

Procesos Tecnológicos y de Información

- **Gestión de sistemas informáticos:** Seguridad de la información, protección de datos, respaldo y recuperación ante desastres.
- **Manejo de software de inventario y ventas:** Actualización, mantenimiento y capacitación en el uso de sistemas.

Procesos de Cumplimiento Legal y Normativo

- **Cumplimiento de normativas locales y nacionales:** Licencias, permisos, normativas ambientales y laborales.
- **Cumplimiento de normativas de protección de datos:** Políticas de privacidad, manejo de información sensible.

2. Límites temporales, espaciales y organizacionales

Límites Temporales

- El sistema de gestión de riesgos tendrá una **vigencia inicial de un año**, con revisiones y actualizaciones anuales o cuando ocurran cambios significativos en la operación o el entorno.
- El análisis de riesgos incluirá tanto **eventos pasados, presentes y potenciales futuros** que puedan afectar la organización.

Límites Espaciales

- **Cobertura principal:** Sede física ubicada en Quevedo, provincia de Los Ríos, Ecuador.
- **Cobertura secundaria:** Operaciones logísticas de entrega a domicilio dentro del cantón Quevedo hasta provincias convexas.
- **Canales digitales:** Página web, redes sociales y plataformas de venta online administradas por la empresa.

Límites Organizacionales

- **Incluye:** Todo el personal (directivos, administrativos, operativos, ventas, logística), proveedores, socios estratégicos y colaboradores temporales.
- **Excluye:** Actividades tercerizadas fuera del control directo de la empresa (por ejemplo, transporte externo contratado para entregas fuera de la ciudad), salvo que afecten procesos críticos.

- **Incluye:** Todos los activos físicos (inventario, maquinaria, equipos), información digital y procesos de decisión estratégica.

3. Recursos disponibles y recursos necesarios

Recursos Disponibles

- **Recursos Humanos:** 21 empleados capacitados en áreas de ventas, operaciones, administración, marketing y finanzas.
- **Infraestructura:** Local comercial, almacén, equipos de oficina, maquinaria de corte, sistemas de seguridad física.
- **Tecnología:** Software de gestión de inventarios y ventas, página web, presencia en redes sociales, equipos informáticos.
- **Financieros:** Fondos propios para operaciones diarias y pequeñas inversiones en mejoras.
- **Procedimientos básicos:** Protocolos internos de seguridad, manuales operativos y guías de atención al cliente.

Recursos Necesarios (a proponer)

- **Capacitación especializada:** Formación en gestión de riesgos, seguridad de la información y manejo de crisis para todo el personal.
- **Implementación de software especializado:** Herramientas para gestión de riesgos, monitoreo y reporte de incidentes.

- **Consultoría externa:** Apoyo profesional para la implementación y auditoría del sistema de gestión de riesgos según ISO 31000.
- **Recursos para seguridad digital:** Mejora de firewalls, antivirus, sistemas de respaldo y políticas de protección de datos.
- **Presupuesto para simulacros y pruebas:** Realización de simulacros de incidentes (robo, incendio, ciberataque) y evaluación de la respuesta organizacional.
- **Recursos para campañas de concientización:** Materiales y talleres para fortalecer la cultura de gestión de riesgos en todos los niveles.

5.6.3.3. Contextos externo e interno

PROCEDIMIENTO NORMALIZADO DE TRABAJO (PNT)

TÍTULO DEL PNT: Procedimiento para la identificación y análisis del contexto interno y externo.
CÓDIGO: PNT-GR-001
VERSIÓN: 1
FECHA DE ELABORACIÓN: 19/06/2025
ÁREA RESPONSABLE: Gerencia

1: Objetivo

Identificar, analizar y documentar los factores internos y externos que puedan disminuir o afectar la capacidad de la organización para cumplir sus metas.

2: Alcance

Todos los niveles de la empresa Multitableros & herrajes, S.A., tanto empleados y empleadores.

3: Responsables

Responsables de área: Verifican, analizan y comparten todo tipo de información a la gerencia sobre factores específicos.

Gerencia General: Aprueban los resultados del análisis antes realizado.

5.6.3.4. Definición de los criterios de riesgo

Los riesgos que se identifican para que el análisis de riesgos asociados a las operaciones de la empresa Multitableros & Herrajes S.A. Deben clasificarse conforme a los lineamientos establecidos por el directorio para tal fin coma están definidos tres niveles de categorización basado en criterios específicos.

Riesgo bajo: son aquellos que, aunque con una afectación moderada pueden ser abordados con recursos internos del departamento afectado y el apoyo de otras áreas no requieren modificaciones estructurales y su plan de acción debe desarrollarse en un plazo mayor a 2 meses por menor a tres, con un presupuesto que no exceda los $500. Seguido se deben de pisar cada 6 meses, buscando mantenerlos dentro de un nivel adaptable de exposición.

Riesgo medio: engloban situaciones que de no ser gestionadas adecuadamente podrían generar consecuencias adversas para la organización su tratamiento debe ejecutarse en un plazo entre 1 y 2 meses, con una inversión máxima de $500 - $1500. Seguido las estrategias para su gestión pueden incluir medidas de prevención disuasión, aceptación o mitigación, siempre bajo un plan de acción definido este tipo de riesgos, Aunque importantes no deberían llegar a comprometer la continuidad de las operaciones.

Riesgo alto: son eventos que demandan atención inmediata y abordaje más robustos tu tratamiento requieren recursos internos, además de una estructura de soporte adicional. Seguido el

plan de acción debe activarse en un plazo no mayor a 15 días un presupuesto asignado de hasta $1500. Seguido su seguimiento deberá realizarse mensualmente y cualquier cambio debe ser documentado y evaluado para una posible categorización. Seguido dado el nivel de amenaza como se recomienda considerar estrategias como compartir o transferir el riesgo

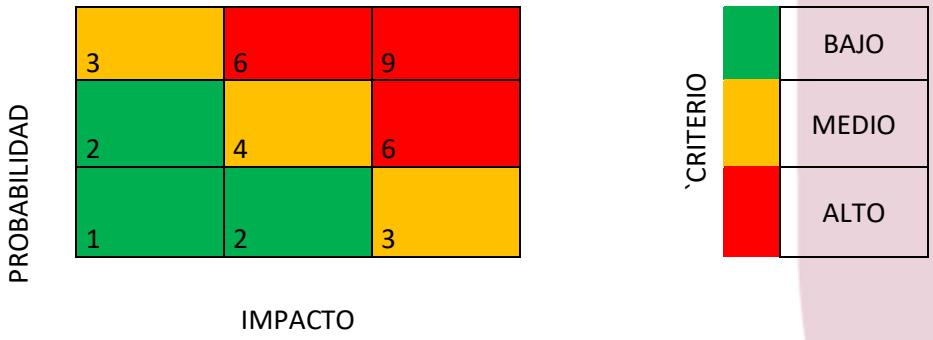
La clasificación de los riesgos en estos tres grupos permite determinar su nivel de criticidad considerando tanto el apetito de riesgo como la capacidad de tolerancia de la empresa todos los riesgos genéticos identificados deben darse dentro de esta categoría lo que facilitará la eliminación de los planes de acción más adecuada.

Para optimizar la gestión, riesgos deben ser organizados según su frecuencia o probabilidad de ocurrencia al nivel de impacto esperado, es decir, las consecuencias potenciales que su materialización podrían provocar acto seguido esta evaluación cuantitativa permitirán priorizar los riesgos como planificar su tratamiento en función de los tiempos de respuesta requeridos como destinar los recursos presupuestarios correspondientes para su investigación efectiva.

Para evaluar los riesgos, se definirá la siguiente matriz.

Figura 15

Apetito de tolerancia del Riesgo para Multitableros & Herrajes S.A.



Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Tabla 29

Matriz de criterios

Criterio	Escala
Probabilidad	Baja (ocasional) / Media (posible) / Alta (frecuente)
Impacto económico	Bajo (< $500), Medio ($500-$1.500), Alto (> $1.500)
Impacto operativo	Sin afectación / Demora leve / Interrupción grave
Impacto en imagen	Interno / Reclamos leves / Pérdida de clientes o reputación

Fuente: *Elaboración propia para Multitableros & Herrajes S.A.*

Riesgo evaluado:

Riesgo: Error en entrega de productos al cliente.

Probabilidad: Media

Impacto económico: Medio

Impacto en imagen: Moderado

Clasificación: Riesgo medio → requiere control inmediato con doble verificación.

Procedimiento Normalizado de Trabajo PNT (Anexo 5)

5.6.4. Evaluación del riesgo

5.6.4.1. Generalidades

Para estandarizar la gestión de riesgos en Multitableros & Herrajes, S.A., se adopta una metodología combinada de probabilidad e impacto, basada en tres niveles de criticidad (bajo, medio y alto). Esta metodología facilita la comparabilidad, priorización y toma de decisiones ejecutivas. En casos

específicos, se podrá usar una metodología alternativa técnicamente sustentada y reconocida internacionalmente.

Los riesgos serán evaluados a través de una combinación de criterios cualitativos y cuantitativos, considerando variables como impacto económico, operativo, legal, reputacional y de seguridad, ajustados a los procesos logísticos y comerciales de la organización.

Tabla 30

Matriz de criterios

Nivel	Probabilidad	Impacto
6 - 9	Alto	Grave
3 - 4	Medio	Moderado
1 – 2	Bajo	Leve

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

La empresa ha definido que su apetito al riesgo es crítico, es decir se encuentra en nivel 5, por lo tanto, todos los riesgos cuyo nivel de riesgo (producto de la probabilidad por la ocurrencia), se encuentre valorado a partir de 5 serán considerados para tratamiento.

5.6.4.2. Identificación del riesgo

En la siguiente tabla se indican todos los riesgos asociados al alcance del sistema de gestión de riesgos a implementarse en la empresa Multitableros & Herrajes S.A.:

Tabla 31

Matriz de Identificación de Riesgos

Tipo de Riesgo	Riesgo Específico
Talento Humano	Falta de personal calificado / rotación alta
Seguridad Informática	Acceso no autorizado / pérdida de información
Infraestructura	Fallas eléctricas / colapsos de sistema logístico
Distribución y Entregas	Interrupción por fallas de transporte / congestión

Reputación y Ética	Comportamiento no ético / atención inadecuada al cliente
Ambiente Externo	Cambios normativos / disturbios sociales / crimen en zonas cercanas
Fraude y Pérdidas	Malversación / robo de inventario o efectivo

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

5.6.4.3. Análisis del riesgo

Tabla 32

Criterios para la evaluación de probabilidad

Valor	Tipo	Descripción
5	Muy Alta	El evento ocurre frecuentemente. Ya ha sucedido o está ocurriendo.
4	Alta	Alta posibilidad; condiciones propicias; amenazas directas o antecedentes similares.
3	Media	Puede ocurrir en ciertas condiciones. Ha pasado a otras empresas similares.
2	Baja	Evento poco probable; sin antecedentes creíbles en la empresa.
1	Muy Baja	Evento extremadamente improbable. No hay antecedentes ni condiciones propicias.

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Tabla 33

Criterios para la evaluación del impacto

Valor	Tipo	Descripción
5	Crítico	Muerte, pérdida financiera > $20,000, pérdida de marca o reputación severa y sostenida.
4	Alto	Lesiones graves, pérdidas entre $9,000 y $10,000, daño reputacional notable.
3	Medio	Lesiones leves, pérdida de $5,000–$9,000, afectación reputacional temporal.
2	Bajo	Primeros auxilios, pérdida menor < $5,000, impacto comercial leve.
1	Muy Bajo	Sin daño humano ni económico considerable.

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Tabla 34

Matriz de Riesgos (Probabilidad x Impacto)

Probabilidad \ Impacto	1 (Muy Bajo)	2 (Bajo)	3 (Medio)	4 (Alto)	5 (Crítico)
5 (Muy Alta)	5	10	15	20	25
4 (Alta)	4	8	12	16	20
3 (Media)	3	6	9	12	15
2 (Baja)	2	4	6	8	10
1 (Muy Baja)	1	2	3	4	5

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

Clasificación de Riesgo:

- 1–5 = Muy Bajo
- 6–10 = Bajo
- 11–15 = Medio
- 16–20 = Alto
- 21–25 = Crítico

5.6.4.4. Valoración del riesgo

En esta etapa, se priorizan los riesgos evaluados y se asigna una clasificación con base en su valor de probabilidad x impacto. A continuación, se presenta una tabla modelo adaptada a los riesgos más relevantes para Megatableros & Herrajes S.A.:

Fórmula:
Valor de riesgo = Probabilidad x Impacto

Tabla 35

Valoración de riesgos – Ferretería megatableros & Herrajes S.A.

Tipo de Riesgo	Riesgo Específico	Prob.	Impacto	Valor	Clasificación
Personal	Consumo de drogas	5	3	15	Medio
Personal	Comportamiento no ético	5	4	20	Alto
Seguridad Ocupacional	Accidentes industriales	3	3	9	Medio
Entorno	Criminalidad en zona	5	4	20	Alto
Infraestructura TIC	Falla del servidor	5	3	15	Medio
Información	Acceso no autorizado a documentos	4	3	12	Medio
Legal/Regulatorio	Prácticas contables inapropiadas	2	5	10	Bajo
Reputación / Cliente	Manejo deficiente de quejas	5	4	20	Alto
Comercial / Producto	Falla de desempeño del producto	5	4	20	Alto
Fraude	Soborno / Malversación	4	5	20	Crítico

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

5.6.5. Tratamiento del riesgo

5.6.5.1. Generalidades

El tratamiento de riesgos consiste en seleccionar e implementar opciones para reducir, eliminar, compartir o aceptar riesgos, conforme a su nivel de criticidad y al contexto operacional de la ferretería.

5.6.5.2. Selección de las opciones para el tratamiento del riesgo

Opciones disponibles:

- Evitar: Suspensión de actividades que impliquen riesgos inaceptables.
- Reducir: Mejora de controles y capacitación.
- Transferir: Seguros, subcontrataciones, contratos con cláusulas de responsabilidad.
- Aceptar: Riesgos menores asumidos con seguimiento interno.

5.6.5.3. Preparación e implantación de los planes de tratamiento del riesgo

Cada riesgo tratado debe tener un Plan de Acción, que incluye:

- Actividades específicas
- Responsables
- Plazo de ejecución
- Indicadores de control

- Documentos de soporte (formatos, checklists, registros)

5.6.6. Seguimiento y revisión

La gestión de riesgos en la ferretería *Megatableros & Herrajes S.A.* es dinámica. En el contexto actual de operaciones (ventas, inventario, logística, atención al cliente, seguridad de la información, etc.), los riesgos evolucionan, lo que exige un proceso continuo de seguimiento y revisión para:

- Validar la eficacia de las medidas de control.
- Adaptar nuevas acciones según los cambios del entorno.
- Generar una cultura organizacional de mejora continua.

Tabla 36

Responsables del seguimiento y revisión

Encargado	Responsabilidad	Objetivo	Frecuencia
Auditores del Sistema de Gestión	Verificación del cumplimiento de controles, hallazgos y documentación objetiva.	Asegurar la trazabilidad del riesgo y retroalimentar a la dirección.	Anual
Gerente General / Gerencia Operativa	Supervisión general de riesgos críticos.	Minimizar impacto en áreas sensibles del negocio.	Trimestral
Sección de Logística y Bodega	Control de riesgos en almacenamiento, entrega y recepción.	Verificar cumplimiento de normas de seguridad y prevención.	Mensual
Personal Operativo y de Ventas	Notificar riesgos o incidentes.	Fomentar la participación activa en el control del riesgo.	Permanente (a demanda)

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

5.6.7. Registro e informe

5.6.7.1. Medios de comunicación

La transparencia en la gestión de riesgos se fortalece con el registro y la comunicación efectiva. Toda la información será documentada, analizada y compartida con las partes interesadas.

Tabla 37

Medios de comunicación

Medio	Objetivo	Público Objetivo
Mapa de Riesgos Físico y Digital	Visualización clara y accesible de riesgos por zonas (bodega, área de corte, caja, oficinas).	Todo el personal
Correo electrónico institucional	Comunicar medidas, hallazgos y recomendaciones de mejora.	Personal interno
Descriptivos de Cargo con Riesgos Inherentes	Incorporar riesgos específicos al perfil de cada rol.	Recursos Humanos y empleados
Carteleras Informativas	Recordatorios visuales de buenas prácticas y riesgos clave.	Área logística, showroom
Socializaciones (charlas, reuniones)	Explicar procedimientos, simulacros y actualizaciones.	Todo el personal
Reuniones comunitarias	Minimizar impactos externos y coordinar seguridad perimetral.	Vecinos, autoridades locales
Inspecciones y visitas técnicas	Verificar la aplicación de controles de riesgo en campo.	Supervisores, auditores
Capacitaciones en gestión de riesgos	Fortalecer la cultura preventiva y la correcta reacción.	Todo el personal operativo
Formación técnica y simulacros	Reacción ante siniestros, primeros auxilios, emergencias.	Personal de logística y seguridad

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

5.6.7.2. Cronograma de actividades para la implementación de procesos de mejora ante los riesgos detectados

Tabla 38

Cronograma de actividades

Actividad	Involucrados	Fecha Estimada
Presentación del proyecto y riesgos priorizados	Dirección General, Jefaturas, Asesores externos	Julio 2025

Presupuesto para la implementación	Dirección, Finanzas	Agosto 2025
Difusión del modelo ISO 31000 y procedimientos	Dirección, Consultores, Operaciones	Agosto – septiembre 2025
Formación de equipo interno de riesgos	Jefaturas de área, Recursos Humanos	Septiembre 2025
Instalación de dispositivos de seguridad, cámaras, GPS, sensores	Sistemas, Seguridad, Logística	Octubre – noviembre 2025
Ejecución de simulacros y testeo de planes de emergencia	Seguridad industrial, Personal	Noviembre 2025
Auditoría interna y revisión de eficacia	Consultores externos, Gerencia	Diciembre 2025
Plan de mejora continua y seguimiento	Dirección, Consultores, Personal clave	Enero – diciembre 2026

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

5.6.8. Auditoría interna

5.6.8.1. Objetivos de la Auditoría interna

- **Verificar que las opciones de tratamiento de riesgos identificadas sean efectivas y prácticas**, es decir, que realmente reduzcan los riesgos a niveles aceptables y puedan ser implementadas en el contexto real de la empresa.
- **Evaluar el cumplimiento de los procesos y controles establecidos en el manual de gestión de riesgos**, asegurando su alineación con la política y los objetivos estratégicos definidos por la organización.
- **Detectar desviaciones, no conformidades y oportunidades de mejora** en la gestión de riesgos, promoviendo la mejora continua y la resiliencia organizacional.

5.6.8.2. Procesos de la Auditoría interna

1. Planificación

- **Definición del alcance:**

  La auditoría abarcará todos los procesos críticos y áreas identificadas en el sistema de gestión de riesgos: inventario, ventas, atención al cliente, almacenamiento, recursos humanos, seguridad física y tecnológica.

- **Criterios de auditoría:**

  - Cumplimiento de la política de gestión de riesgos.
  - Aplicación de controles y medidas de tratamiento según la matriz de riesgos.
  - Cumplimiento de normativas legales y estándares ISO 31000.

- **Cronograma:**

  - Preparación documental: 1 semana.
  - Auditoría en terreno y entrevistas: 3 días.
  - Emisión de informe preliminar: 3 días posteriores.
  - Seguimiento de acciones correctivas: 1 mes después del informe final.

2. Ejecución

- **Revisión documental:**

  - Manual de gestión de riesgos.
  - Matriz de riesgos y controles implementados.

- Registros de incidentes, reportes de accidentes y simulacros.
- Políticas y procedimientos internos.

- **Entrevistas:**
  - Gerente General.
  - Responsables de área (ventas, operaciones, RRHH, TI).
  - Personal operativo y administrativo.

- **Evaluaciones en terreno:**
  - Verificación de la existencia y uso de controles físicos (extintores, CCTV, cerraduras, señalización de rutas de evacuación).
  - Observación del cumplimiento de protocolos de seguridad y medidas tecnológicas (antivirus, backups, firewalls).
  - Simulación de situaciones de riesgo (por ejemplo, simulacro de incendio o intento de acceso no autorizado).

3. Informe

- **Estructura del informe:**
  - **Resumen ejecutivo:** Principales hallazgos y conclusiones.
  - **Hallazgos positivos:** Controles efectivos, buenas prácticas observadas.

- **Observaciones:** Áreas donde los controles pueden ser mejorados.
- **No conformidades:** Incumplimientos respecto a procedimientos, controles o requisitos legales.
- **Recomendaciones:** Acciones correctivas y preventivas sugeridas.

- **Ejemplo de hallazgos:**
  - Se detectó que el sistema de backups automáticos funciona correctamente, pero los simulacros de recuperación de datos no se realizan con la frecuencia recomendada.
  - El acceso físico a la bodega no está debidamente restringido fuera de horario laboral.
  - El personal conoce los procedimientos de emergencia, pero no todos han participado en simulacros recientes.

4. Seguimiento

- **Verificación de acciones correctivas:**
  - Se establece un plan de acción con responsables y fechas límite para subsanar las no conformidades detectadas.
  - Se realiza una revisión de seguimiento (presencial o documental) para comprobar la implementación efectiva de las mejoras.
  - Se documentan los resultados y, si es necesario, se ajustan los procedimientos o se programan nuevas capacitaciones.

Modelo de Auditoría Interna ISO 31000:2018 de Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. (Ver Anexo 9).

5.6.8.3. No conformidades y acciones correctivas

Las no conformidades detectadas durante la auditoría interna deben ser clasificadas según su nivel de impacto y deben contar con un plan de acción correctivo detallado.

Tabla 39

Registro de No conformidades y acciones correctivos

Código NC	Área	Descripción de la NC	Clasificación	Acción Correctiva	Responsable	Fecha Límite	Seguimiento
NC-001	**Logística**	**Falta de señalización de riesgo físico**	**Mayor**	**Colocar señalética en áreas críticas**	**Jefe de Bodega**	**15/07/2025**	**22/07/2025**
NC-002	**TIC**	**No se realiza respaldo semanal de información**	**Crítica**	**Programar respaldos automáticos**	**Jefe de Sistemas**	**20/07/2025**	**27/07/2025**
NC-003	**Atención Cliente**	**No se registra formalmente las quejas recibidas**	**Menor**	**Implementar bitácora digital de quejas**	**Supervisor Comercial**	**18/07/2025**	**25/07/2025**
NC-004		**Falta de simulacros de recuperación de datos**	**Mayor**	**Programar y ejecutar simulacros de recuperación de datos cada 6 meses. Documentar los resultados.**	**Jefe de Sistemas**	**25/07/2025**	**25/08/2025**
NC-005		**Acceso físico no restringido a la bodega fuera de**	**Mayor**	**Instalar sistema de control de acceso con registro de**	**Recursos Humanos**	**20/07/2025**	**21/07/2025**

	horario laboral		**ingresos. Capacitar al personal sobre su uso.**			
NC-006	**Personal no ha participado en simulacros recientes**	**Mayor**	**Planificar y ejecutar simulacros trimestrales incluyendo a todo el personal. Emitir constancia de participación.**	**Recursos Humanos**	**02/07/2025**	**02/09/2025**
NC-007	**Ausencia de verificación de la eficacia de ciertos controles tecnológicos**	**Mayor**	**Coordinar auditoría externa de seguridad informática. Incluir prueba de firewalls, antivirus y backups.**	**Jefe de sistemas**	**15/07/2025**	**15/08/2025**
NC-008	**Inexistencia de registro de mantenimiento de extintores**	**Menor**	**Contratar empresa certificada para mantenimiento. Registrar las inspecciones y colocar etiquetas visibles en los equipos.**	**Recursos humanso**	**02/07/2025**	**02/047/2026**

Fuente: *Elaboración propia para Multitableros & Herrajes S.A*

CAPITULO 6

6. CONCLUSIONES Y APLICACIONES

6.1. Conclusiones generales

El desarrollo de este proyecto representa para nuestro equipo una experiencia enriquecedora y de gran valor profesional. A través de un sistema de gestión de riesgos basado en la norma ISO 31000:2018, logramos proporcionar a la empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A. una herramienta útil y aplicable a su realidad operativa, que le permitirá enfrentar de forma estructurada y proactiva los distintos riesgos que puedan amenazar su continuidad.

Uno de los principales logros es haber involucrado activamente a todos los niveles de la organización, promoviendo una cultura de gestión de riesgos como una responsabilidad compartida y no limitada a un solo departamento. Esta participación consiste en generar conciencia sobre la importancia de anticiparse a posibles amenazas y actuar con oportunidad y eficacia.

Consideramos que los objetivos planteados al inicio del proyecto se constituyen a cabalidad con el enfoque de un diseño de implementación de procesos claros y obligatorios para la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos, sentando las bases para una gestión integrada y transversal que contribuya a la sostenibilidad de la empresa en el tiempo.

6.2. Conclusiones específicas

6.2.1. Análisis del cumplimiento de los objetivos de la investigación

A lo largo del desarrollo de este trabajo, se logran cumplir con los objetivos específicos propuestos al inicio de la investigación, centrados en la elaboración de un manual de gestión de riesgos basado en la norma ISO 31000:2018, y no en la implementación operativa del sistema.

En primer lugar, se identifican, analizan y evalúan los riesgos relevantes presentes en las actividades y funciones significativas de la empresa, considerando tanto amenazas como oportunidades. Esta tarea se realiza mediante el estudio detallado de los procesos de la organización, la caracterización de eventos de riesgo y la estimación de su probabilidad e impacto, lo cual permite priorizarlos adecuadamente.

En segundo lugar, el manual propuesto establece lineamientos y procedimientos claros para prevenir, detectar y responder a riesgos relacionados con la seguridad de la información. A través del enfoque propuesto, se fortalecen los mecanismos de protección de los activos informáticos, incluyendo datos, sistemas e infraestructura tecnológica, alineados con buenas prácticas internacionales.

Asimismo, se aborda la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información, incorporando en el manual referencias a las normativas legales vigentes en Ecuador. Esto permitirá a la organización adecuarse al marco regulatorio aplicable y mejorar su nivel de cumplimiento.

Finalmente, se realiza una evaluación integral de los riesgos actuales presentes en la empresa, lo cual sirvió como base para formular un plan de gestión de riesgos orientado a reducir o mitigar los impactos potenciales sobre la organización. Este plan, incluido como parte del manual, contempla acciones específicas, responsables y mecanismos de seguimiento, promoviendo una gestión proactiva.

En conclusión, el trabajo permite alcanzar plenamente los objetivos planteados, al entregar una herramienta técnica y estructurada que servirá como guía para que la empresa gestione sus riesgos de forma sistemática, anticipada y alineada con estándares internacionales, sin que ello implique una implementación inmediata, la cual quedará sujeta a futuras decisiones de la alta dirección.

6.2.2. Contribución a la gestión empresarial

El desarrollo de este proyecto representa un aporte significativo para la empresa, ya que ofrece una base estructurada para una futura gestión de riesgos eficaz, sustentada en los lineamientos de la norma ISO 31000:2018. A través del diseño del manual y de los procedimientos propuestos, se sientan las bases para fortalecer la cadena de valor organizacional, promoviendo una cultura de prevención y mejora continua. Si bien la implementación del sistema no forma parte de los alcances de esta investigación, se considera que su aplicación práctica podrá generar beneficios relevantes en el futuro, siempre que se lleve a cabo con compromiso institucional y se mantenga una actualización constante de los contenidos, formatos y responsables definidos. En este sentido, el proyecto

proporciona una herramienta técnica de gran utilidad que servirá de guía para una posterior toma de decisiones en la empresa.

6.2.3. Contribución a nivel académico

Los conocimientos, la práctica y el desarrollo del sistema de gestión de riesgos no solo contribuye a la empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A., más bien sirve como una guía a futuros alumnos que deseen incursionar en este mundo apasionante de la gestión de riesgos, comprendiendo todo lo que ello implica y dando el valor que realmente requiere una organización en cuanto se refiere a la gestión de riesgos.

6.2.4. Contribución a nivel personal

El desarrollo del presente trabajo ha representado una valiosa experiencia de aprendizaje para todos los integrantes del grupo, permitiéndonos fortalecer nuestras competencias como futuros gestores de riesgos, conforme a los lineamientos establecidos por la Norma ISO 31000:2018. A través del diseño del modelo de gestión de riesgos aplicado a la empresa Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes S.A., logramos no solo comprender los principios fundamentales de la gestión del riesgo, sino también su aplicación práctica mediante la elaboración de procesos, procedimientos y formatos específicos.

Esta experiencia no solo enriquece nuestro conocimiento teórico, sino que también sirve como precedente metodológico para replicar enfoques similares en los diversos sectores en los que cada uno de los integrantes del grupo profesionalmente se desempeña. Al inicio del proyecto, los conocimientos sobre gestión de riesgos eran generales y limitados; sin embargo, a medida que avanzamos en el diseño del modelo y contrastamos nuestras experiencias provenientes de distintas industrias, logramos un aprendizaje colaborativo que potenció la comprensión integral de la gestión de riesgos.

En definitiva, este trabajo ha contribuido significativamente a nuestra formación profesional, al dotarnos de herramientas técnicas y prácticas que serán de gran utilidad en futuros contextos organizacionales donde sea necesario aplicar una gestión de riesgos eficaz y alineada con estándares internacionales.

6.3. Limitaciones a la Investigación

Durante el desarrollo del presente proyecto, orientado al diseño de un sistema de gestión de riesgos basado en la norma ISO 31000:2018, enfrentamos diversas limitaciones que condicionan el alcance del trabajo realizado.

En primer lugar, una de las principales restricciones corresponde al acceso limitado a información formal y documentada por parte de la empresa. Al no contar con un sistema de gestión estructurado ni registros sistematizados de incidentes o eventos de riesgo, debemos basar gran parte del análisis

en observación directa y en entrevistas informales, lo que afecta la precisión y profundidad de los datos recolectados.

Asimismo, el tiempo disponible para la elaboración del proyecto es reducido, lo que nos obliga a priorizar ciertas actividades clave como la identificación y valoración de riesgos y dejar fuera etapas más detalladas del tratamiento o seguimiento. Esta restricción impide el desarrollo de simulaciones o validaciones internas del diseño propuesto.

Otra limitación importante es la disponibilidad del personal de la empresa, quienes colaboran de forma intermitente debido a sus actividades diarias. Esto dificulta mantener una comunicación continua y obtener retroalimentación inmediata sobre los avances del diseño del sistema.

Desde el punto de vista metodológico, debemos adaptar los lineamientos de la norma ISO 31000:2018 al contexto real de una microempresa, lo que implica realizar simplificaciones que, si bien no afectan el propósito del diseño, sí limitan su alcance técnico completo.

Finalmente, es importante señalar que el proyecto culmina con el diseño del sistema, sin avanzar hacia su aplicación operativa, debido a que no forma parte de los objetivos establecidos ni de las capacidades del equipo durante esta etapa. Esta situación restringe la posibilidad de evaluar el funcionamiento real del sistema en el entorno empresarial.

Estas limitaciones se consideran al momento de interpretar los resultados obtenidos y de proponer líneas de acción futuras para una posible implementación.

BIBLIOGRAFÍA

ACESCO. (21 de marzo de 2021). Recuperado el 25 de abril de 2025, de https://acesco.com.ec/wp-content/uploads/2021/09/Politica-Proteccion-de-Datos-Construyamos-Ecuador.pdf

COIP. (10 de febrero de 2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL*. Recuperado el 27 de abril de 2025, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

EMIS. (10 de febrero de 2025). *EMIS*. Recuperado el 22 de abril de 2025, de https://www.emis.com/php/company-profile/EC/Ferreteria_Tableros_-_Herrajes___Afines_Multitableros___herrajes_SA_es_8196893.html

GLOBAL SUITE SOLUTIONS. (19 de octubre de 2023). Recuperado el 20 de abril de 2025, de https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-31000-y-para-que-sirve/

Global Support. (26 de julio de 2022). Recuperado el 26 de abril de 2025, de https://globalsupport.com.ec/2022/07/26/principios-de-la-ley-organica-de-proteccion-de-datos-personales/

ITURAN. (s.f.). Recuperado el 25 de abril de 2025, de https://www.ituran.com.ec/politica-general-de-proteccion-de-datos-personales/

Ley Orgánica de Protección de Datos Personales. (26 de mayo de 2021). Recuperado el 23 de abril de 2025, de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Molina Moreno, A. C., Espitia Mojica, C. A., & Suárez Vargas, N. A. (22 de Mayo de 2022). ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS. *DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS INTEGRADO A PARTIR DEL ESTÁNDAR PMI Y LA NORMA ISO 31000:2018 APLICADO AL PROYECTO PARQUE SOLAR PLANETA RICA EN CÓRDOBA*. La Libertad, Santa Elena, Ecuador. Obtenido de https://repository.universidadean.edu.co/server/api/core/bitstreams/d4e616f9-485e-4f71-8b6b-dad46b1e2a98/content

Multitableros & Herrajes S.A. (2025). *Multitableros & Herrajes S.A.* Recuperado el 21 de abril de 2025, de https://www.multitableros.store/

Pro Sciences. (septiembre de 2024). Recuperado el 26 de abril de 2025, de https://journalprosciences.com/index.php/ps/article/view/753

Rodríguez Quimí, E. L. (28 de Diciembre de 2023). Tesis. *Aplicación de la norma ISO 31000:2018 para mejorar la gestión de riesgos de la empresa Mirapez S.A. cantón Santa Elena, Ecuador.* La Libertad, Santa Elena, Ecuador. Obtenido de https://repositorio.upse.edu.ec/handle/46000/10597

Trujillo Duque Ferreterias. (s.f.). Recuperado el 24 de abril de 2025, de https://www.trujilloduqueferreterias.com.ec/politicas/privacidad

ANEXOS

ANEXO 1

Consentimiento para el tratamiento de mis datos personales

Quevedo, 1 de abril del 2025

Señores:

UNIVERSIDAD INTERNACIONAL DEL ECUADOR

De mis consideraciones:

Por medio de la presente carta, yo López Brito Byron Daniel con cédula 1718968504 les otorgo la autorización a los alumnos de la Universidad Internacional del Ecuador mismos que se encuentran realizando la Maestría en Gestión de Riesgos, para que realicen su trabajo de titulación en el levantamiento de información de la empresa y de esa forma tener la implementación de la norma ISO 31000; 2018 Gestión de Riesgo, en la empresa Ferretería Tableros Herrajes & Afines, Multitableros &Herrajes S.A con RUC 1291767172001.

La razón de esta autorización es para que los alumnos: Diana Carolina Cárdenas Esquivel, Bryan González Ramírez, Kleber Joselito López Brito, Carlos Alfonso Romero Romero, Ricardo Emmanuel Yagual Panchana cursantes de la Maestría en Gestión de Riesgo puedan realizar todo el levantamiento de información de la empresa y puedan desarrollar su plan de titulación, hasta el mes de Julio del 2025.

Por la favorable atención que se digne dar a la presente, desde ya reitero mis debidos agradecimientos.

Reciban un cordial saludo.

Atentamente,

López Brito Byron Daniel

1718968504

Teléfono: 0992315771

Correo: multitablerosyherrajes@gmail.com

ANEXO 2

Mapa de Riesgos – Megamaderas & Herrajes

Se presenta una tabla con los principales riesgos identificados, su nivel de impacto y probabilidad, además de una propuesta de tratamiento:

Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Medida de Control Propuesta
Robo de mercancía o efectivo	Alta	Alto	Crítico	Instalación de CCTV, contratación de servicio de seguridad, control de accesos.
Incendio por fallas eléctricas	Media	Alto	Alto	Mantenimiento eléctrico, extintores y señalética visible, capacitación en emergencias.
Acceso no autorizado a información (correo, inventario)	Alta	Medio	Alto	Uso de contraseñas seguras, autenticación en dos pasos, capacitación en ciberseguridad.
Errores en el despacho de productos	Media	Medio	Medio	Implementación de sistema de control digital de inventario y doble verificación.
Lesiones por manipulación de carga	Media	Medio	Medio	Capacitación en ergonomía y uso correcto de EPP.

Interrupción del servicio de internet	Alta	Bajo	Medio	Uso de respaldo de datos offline y proveedores alternativos de conectividad.
Retrasos de proveedores	Media	Medio	Medio	Diversificación de proveedores, contratos con cláusulas de cumplimiento.
Sismos o desastres naturales	Baja	Alto	Medio	Plan de evacuación, seguros contra siniestros, simulacros.

ANEXO 3

Plan de Acción para la Implementación del Sistema de Gestión de Riesgos

Empresa: Megamaderas & Herrajes – Sucursal Quevedo

Duración estimada: 6 meses

Cronograma por Fases

Fase	Actividad	Responsable	Duración	Fecha estimada	Resultado Esperado
Fase 1	Diagnóstico inicial y análisis de riesgos actuales	Responsable de Seguridad y Riesgos	2 semanas	1 al 15 de julio	Matriz de riesgos preliminar
Fase 2	Formación del Comité de Gestión de Riesgos	Gerente de Sucursal	1 semana	16 al 22 de julio	Comité operativo formalmente
Fase 3	Elaboración del plan de gestión de riesgos (documento base)	Comité de Riesgos	2 semanas	23 de julio al 5 de agosto	Documento del sistema de gestión listo
Fase 4	Diseño de procedimientos y formatos (registro, reporte, respuesta)	Responsable de Seguridad	2 semanas	6 al 19 de agosto	Formatos y protocolos internos disponibles

Fase 5	Capacitaciones a todo el personal (física, digital, emergencias)	Responsable de RR.HH.	3 semanas	20 de agosto al 10 de septiembre	Personal capacitado y sensibilizado
Fase 6	Implementación del sistema y primeros registros de riesgo	Comité de Riesgos	1 mes	11 de septiembre al 10 de octubre	Sistema funcionando en fase piloto
Fase 7	Evaluación del sistema y ajustes	Comité + Gerencia	2 semanas	11 al 25 de octubre	Informe de evaluación con mejoras propuestas
Fase 8	Integración al funcionamiento rutinario	Todos los responsables	Permanente	Desde 26 de octubre en adelante	Sistema completamente activo e integrado

ANEXO 4

Indicadores de Éxito del Plan

- Al menos 1 capacitación general impartida a todos los empleados.
- 100% del personal administrativo y logístico familiarizado con protocolos.
- Matriz de riesgos actualizada cada 2 meses.
- Comité de riesgos activo y con actas mensuales.
- Reducción de incidentes operativos o de seguridad reportados.

Formato 1: Registro de Identificación y Evaluación de Riesgos

Campo	**Descripción / Ejemplo**
ID del Riesgo	R-001
Fecha de identificación	2025-06-01
Área / Departamento	Almacén / Logística
Descripción del Riesgo	Robo de mercancía debido a falta de vigilancia
Causa(s)	Falta de cámaras y control de accesos
Consecuencia(s)	Pérdida económica, retrasos en entregas
Probabilidad	Alta / Media / Baja
Impacto	Alto / Medio / Bajo
Nivel de riesgo	Crítico / Alto / Medio / Bajo (combinación de probabilidad e impacto)
Responsable de seguimiento	Responsable de Seguridad

Medidas de control actuales	Guardia nocturno, candados
Medidas propuestas / nuevas	Instalación de CCTV, control de accesos
Estado	Abierto / En proceso / Cerrado
Comentarios / Observaciones	Se debe evaluar presupuesto para cámaras

Formato 2: Registro de Seguimiento y Control de Riesgos

ID del Riesgo	**R-001**
Fecha de seguimiento	2025-07-01
Acción realizada	Instalación de 3 cámaras de seguridad
Resultado	Reducción de incidentes reportados
Comentarios	Personal capacitado para monitoreo
Responsable	Responsable de Seguridad
Fecha próxima revisión	2025-08-01
Estado	En proceso / Cerrado

Formato de Reporte de Incidentes

Campo	**Descripción / Ejemplo**
ID del Incidente	INC-001

Fecha y hora del incidente	2025-06-15, 14:30
Lugar / Área	Almacén
Persona que reporta	Juan Pérez
Descripción del incidente	Robo de mercancía detectado en inventario
Tipo de incidente	Seguridad física / Robo / Otro
Consecuencias	Pérdida de productos, retrasos en entregas
Medidas inmediatas tomadas	Reporte a seguridad, revisión de cámaras
Persona(s) involucrada(s)	N/A
Estado del incidente	Abierto / En proceso / Cerrado
Comentarios adicionales	Se iniciará investigación interna

Formato de Plan de Acción para Gestión de Riesgos

Campo	**Descripción / Ejemplo**
ID del Plan	PA-001
Riesgo asociado	Robo de mercancía
Descripción de la acción	Instalación de sistema de CCTV
Responsable(s)	Responsable de Seguridad
Recursos necesarios	Presupuesto para cámaras y equipo de monitoreo
Fecha de inicio	2025-07-01
Fecha de fin estimada	2025-07-31

Estado	Pendiente / En progreso / Completado
Indicadores de éxito	Reducción en incidentes reportados en un 80%
Comentarios	Coordinar con proveedor local para instalación

ANEXO 5

Procedimiento Normalizado de Trabajo (PNT)

FERRETERÍA MULTITABLEROS & HERRAJES S.A.	**PROCEDIMIENTO GENERAL**	**Código**	PNT-ENT-001
	PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	**Versión**	1
		Fecha emisión	18/6/2025
		Área	Despacho
		Fecha edición	18/6/2025
		Revisión	Anual
Procedimientos relacionados:			

PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO

ÍNDICE

1. Objetivo

2. Alcance

3. Responsables

4. Materiales y herramientas necesarias

5. Riesgos identificados

6. Procedimiento paso a paso

7. Indicadores de desempeño (KPI)

8. Control y revisión del PNT

9. Anexo sugeridos

Redactado por:	**Revisado por:**	**Aprobado por:**

PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	Código	PNT-ENT-001
	Página	2 de 6
	Fecha	18/6/2025

1. Objetivo

Garantizar que la entrega de productos al cliente se realice con precisión, seguridad y en el tiempo acordado, minimizando errores, reclamos y pérdidas materiales.

2. Alcance

Aplica al personal encargado de la preparación, revisión y despacho de productos vendidos para ser entregados directamente al cliente, ya sea en el local o a domicilio.

3. Responsables

- **Despachador o bodeguero:** Alista y entrega correctamente los productos.
- **Cajero(a):** Verifica que la factura esté emitida y pagada.
- **Chofer (si aplica):** Asegura el transporte seguro y firma de recepción.
- **Jefe de Bodega:** Supervisa cumplimiento del procedimiento.

4. Materiales y herramientas necesarias

- Factura o nota de venta
- Lista de despacho
- Carretilla o equipo de carga
- Hoja de verificación de entrega (Anexo 7)
- Vehículo (si es entrega externa) (Anexo 8)
- Dispositivo para toma de fotos o evidencia de entrega (Anexo 9)

PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	Código	PNT-ENT-001
	Página	3 de 6
	Fecha	18/6/2025

5. Riesgos identificados

Código	Riesgo	Nivel	Tratamiento
R-001	Entrega incompleta	Alto	Verificación con check-list y firma
R-002	Producto equivocado entregado	Medio	Revisión cruzada con factura
R-003	Daño del producto en traslado	Medio	Embalaje adecuado y fijación en transporte
R-004	Entrega a persona equivocada	Bajo	Solicitar cédula o firma del receptor
R-005	Retraso en la entrega	Medio	Confirmación anticipada de dirección y hora

PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	**Código**	PNT-ENT-001
	Página	4 de 6
	Fecha	18/6/2025

6. Procedimiento paso a paso

Paso	Actividad
1	Confirmar que la factura ha sido emitida y pagada.
2	Verificar que el detalle del producto coincida con la factura.
3	Buscar y reunir los productos correspondientes.
4	Revisar cantidad, tipo, estado físico y empaque.
5	Completar **lista de verificación** con cada ítem entregado (checklist).
6	Realizar la entrega: - Si es en tienda: entregar directamente y solicitar firma. - Si es a domicilio: cargar productos al vehículo, asegurar y trasladar.
7	Tomar evidencia de entrega (foto con el cliente o firma en formato físico).
8	Archivar hoja de entrega firmada y registrar en bitácora diaria de despacho.
9	En caso de reclamo o incidente, informar al jefe de bodega y documentar en reporte.

PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	Código	PNT-ENT-001
	Página	5 de 6
	Fecha	18/6/2025

7. Indicadores de desempeño (KPI)

Indicador	Meta mensual
Porcentaje de entregas sin error	≥ 97%
Tiempo promedio de entrega	≤ 4 horas (dentro de Quevedo)
Incidentes por daño o pérdida	≤ 2 por mes

8. Control y revisión del PNT

- Responsable: jefe de Bodega
- Revisión: Cada 12 meses o ante cambio del proceso/logística
- Verificación: Revisión semanal de 5 entregas aleatorias

9. Anexos sugeridos

- Formato de checklist de entrega
- Hoja de recepción de cliente (con firma)
- Mapa de riesgos del proceso de despacho

PROCEDIMIENTO DE ELABORACIÓN DE UN PROCEDIMIENTO NORMALIZADO DE TRABAJO	Código	PNT-ENT-001
	Página	6 de 6
	Fecha	18/6/2025

Aplicación del enfoque ISO 31000:2018

Principio ISO 31000	Aplicación en el procedimiento
Integración	Involucra facturación, bodega y transporte de forma coordinada
Estructura y cultura	Se definen roles, responsabilidades y controles claros
Evaluación continua	Uso de indicadores, revisión de errores y mejoras periódicas
Toma de decisiones	El procedimiento sirve como guía para actuar con base en evidencia

ANEXO 6

Formato de Checklist de Entrega

FERRETERÍA MULTITABLEROS & HERRAJES S.A.
Checklist de Verificación para Entrega de Productos

Fecha de entrega:	**N° de factura:** _____
Cliente:	Teléfono: _____
Dirección de entrega: _____	
Responsable de despacho: _____	

Lista de productos entregados

N°	Código del producto	Descripción	Cantidad Facturada	Cantidad Entregada	Estado	Observaciones
1					[] OK [] Dañado	
2					[] OK [] Dañado	
3					[] OK [] Dañado	
4					[] OK [] Dañado	

Tipo de entrega:

☐ En tienda ☐ A domicilio

Observaciones generales:

_____

_____

Verificado por:

Nombre: _____ Firma: _____

Entregado por:

Nombre: _____ Firma: _____

ANEXO 7

Hoja de Recepción del Cliente (con firma)

FERRETERÍA MULTITABLEROS & HERRAJES S.A.
Hoja de Confirmación de Recepción de Productos

Fecha de entrega: _____	**Hora: _____**
Cliente: _____	
Dirección de entrega: _____	
Factura / Remisión N°: _____	
Monto total: $_____	

Resumen de productos entregados:

N°	Código	Descripción	Cantidad	Observaciones (si aplica)
1				
2				
3				

El cliente declara que ha recibido los productos indicados en buen estado y en la cantidad señalada.

🖉 **Firma del cliente receptor:**
Nombre completo: _____
Cédula/RUC: _____
Firma: _____
Teléfono de contacto: _____

🚚 **Entregado por (nombre del colaborador):**
Nombre: _____ Firma: _____

ANEXO 8

Mapa de Riesgos del Proceso de despacho

FERRETERÍA MULTITABLEROS & HERRAJES S.A.
Mapa de Riesgos – Proceso de Entrega de Productos

N°	Etapa del proceso	Riesgo identificado	Probabilidad	Impacto	Nivel de Riesgo	Medida de control aplicada
1	Preparación del pedido	Error en la selección del producto	Media	Alto	**Alto**	Doble verificación con factura
2	Carga del vehículo	Daño al producto por mala manipulación	Alta	Medio	**Alto**	Uso de carretillas y embalaje adecuado
3	Transporte a domicilio	Retraso por tráfico o dirección incorrecta	Media	Bajo	**Medio**	Confirmación previa de dirección
4	Entrega al cliente	Producto entregado a persona incorrecta	Baja	Alto	**Medio**	Solicitar cédula o firma de receptor
5	Registro post-entrega	No se archiva evidencia	Media	Bajo	**Medio**	Checklist + hoja de recepción firmada

Leyenda del nivel de riesgo:

- 🔴 **Alto** = Acción inmediata
- 🟠 **Medio** = Control y monitoreo
- 🟢 **Bajo** = Registro y seguimiento eventual

ANEXO 9

Modelo de Auditoría Interna ISO 31000:2018

Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.

1. Propósito

Definir el proceso para planificar, ejecutar, documentar y dar seguimiento a auditorías internas del Sistema de Gestión de Riesgos (SGR), evaluando su conformidad con la norma ISO 31000:2018 y la eficacia de la gestión de riesgos en la organización.

2. Alcance

Este procedimiento aplica a todas las áreas, procesos y actividades relacionadas con la gestión de riesgos dentro de la empresa.

3. Responsabilidades

- **Equipo Auditor**:
  - Realizar la auditoría conforme al procedimiento.
  - Recopilar evidencias objetivas.
  - Elaborar el informe de auditoría.
- **Auditor Líder**:
  - Coordinar la auditoría y supervisar al equipo auditor.
  - Presentar los resultados a la alta dirección.
- **Responsables de Áreas Auditadas**:
  - Facilitar el acceso a información y documentación.
  - Implementar las acciones correctivas y de mejora identificadas.

4. Definiciones

- **Auditoría Interna**: Proceso independiente y documentado para evaluar la conformidad del SGR con los requisitos establecidos y su eficacia.
- **No Conformidad**: Incumplimiento de un requisito del SGR o de la ISO 31000:2018.
- **Acción Correctiva**: Medida tomada para eliminar la causa de una no conformidad.

- **Evidencia Objetiva**: Registros, declaraciones de hechos u otra información que demuestre la conformidad o no conformidad.

5. Proceso de Auditoría Interna

5.1. Planificación

- **Definir el alcance**: Seleccionar procesos, áreas y actividades a auditar (ejemplo: gestión de inventarios, seguridad de la información, ventas, recursos humanos).
- **Establecer los criterios de auditoría**: Basados en la política de gestión de riesgos, procedimientos internos y requisitos de ISO 31000:2018.
- **Elaborar el cronograma de auditoría**: Fechas, responsables y recursos necesarios.
- **Comunicación**: Informar a las áreas auditadas sobre el alcance y objetivos.

5.2. Ejecución

- **Revisión documental**: Políticas, procedimientos, matrices de riesgos, registros de incidentes, controles implementados.
- **Entrevistas**: Con responsables de área y personal clave.
- **Observación en terreno**: Verificación de controles físicos, tecnológicos y operativos.
- **Recopilación de evidencias**: Documentos, registros, observaciones y testimonios.

5.3. Informe

- **Redacción del informe**:
    - Resumen ejecutivo.
    - Hallazgos positivos.
    - Observaciones.
    - No conformidades.
    - Recomendaciones de mejora.
- **Presentación a la dirección**: Entrega formal del informe y discusión de los hallazgos.

5.4. Seguimiento

- **Plan de acción**: Establecer responsables y plazos para la implementación de acciones correctivas.

- **Verificación de cierre**: Revisar la ejecución de las acciones y su eficacia.
- **Registro**: Mantener evidencia documental del seguimiento y cierre de no conformidades.

6. Estructura del Informe de Auditoría

Sección	Contenido
Resumen Ejecutivo	Principales hallazgos y conclusiones.
Alcance y Objetivos	Qué se auditó, bajo qué criterios y por qué.
Desarrollo de la Auditoría	Detalle de actividades realizadas, áreas visitadas, entrevistas hechas.
Hallazgos	Conformidades, no conformidades y observaciones.
Recomendaciones	Acciones sugeridas para corregir y mejorar el SGR.
Plan de Acciones	Tabla con responsables, plazos y estado de cada acción correctiva.

7. Ejemplo de Tabla de Seguimiento

Hallazgo/No Conformidad	Acción Correctiva	Responsable	Fecha Límite	Estado
Falta de simulacro de backup	Programar simulacros trimestrales	Responsable TI	30/06/2025	Pendiente
Acceso libre a bodega fuera de horario	Instalar cerraduras electrónicas	Jefe de Operaciones	15/07/2025	En proceso
Personal sin capacitación reciente	Realizar capacitación y simulacro	RRHH	10/07/2025	Pendiente

8. Mejora Continua

- Programar auditorías internas periódicas (al menos una vez al año o ante cambios importantes).
- Actualizar los procedimientos y controles según los resultados de las auditorías.
- Fomentar la cultura de gestión de riesgos y la participación de todo el personal.

9. Anexos

- Lista de verificación (checklist) de conformidad con ISO 31000:2018.
- Formatos de informe de auditoría y plan de acción.
- Evidencias recopiladas (registros, fotografías, actas de entrevistas).

Checklist de Auditoría Interna

ISO 31000:2018 – Gestión de Riesgos
Empresa: Ferretería Tableros Herrajes & Afines, Multitableros & Herrajes, S.A.
Fecha: _____
Auditor: _____
Área Auditada: _____

Nº	Ítem de Verificación	Cumple	No Cumple	No Aplica	Observaciones/Evidencia
1	¿Existe una política de gestión de riesgos documentada y comunicada?	☐	☐	☐	
2	¿Se identifican y actualizan los riesgos en todas las áreas clave de la empresa?	☐	☐	☐	
3	¿Se cuenta con una matriz de riesgos vigente y revisada periódicamente?	☐	☐	☐	
4	¿Están definidos los responsables de la gestión de riesgos por área/proceso?	☐	☐	☐	
5	¿Se encuentran implementadas medidas de control y tratamiento para los riesgos identificados?	☐	☐	☐	
6	¿Se han realizado simulacros o pruebas de los controles	☐	☐	☐	

	críticos (ej. backups, accesos, evacuación)?			
7	¿El personal ha sido capacitado en gestión de riesgos y procedimientos de seguridad?	☐	☐	☐
8	¿Se registran y analizan los incidentes o eventos asociados a riesgos?	☐	☐	☐
9	¿Existen procedimientos para la revisión y mejora continua del sistema de gestión de riesgos?	☐	☐	☐
10	¿Se han implementado acciones correctivas ante no conformidades detectadas en auditorías previas?	☐	☐	☐
11	¿Se cumple con los requisitos legales y normativos aplicables en materia de gestión de riesgos?	☐	☐	☐
12	¿La alta dirección revisa y apoya el sistema de gestión de riesgos?	☐	☐	☐
13	¿Se mantiene evidencia documental de todas las actividades de gestión de riesgos?	☐	☐	☐

ANEXO 10

Modelo de No Conformidades y Acciones Correctivas

Empresa: Ferretería Multi Tableros & Herrajes S.A.
Ubicación: Quevedo
Norma Base: ISO 31000:2018 – Gestión del Riesgo

1. Objetivo

Establecer un procedimiento de gestión de no conformidades y acciones correctivas basado en principios de gestión del riesgo, con el fin de **eliminar o reducir los impactos negativos** derivados de fallos en procesos, seguridad, calidad o cumplimiento dentro de las operaciones de la ferretería.

2. Alcance

Este procedimiento aplica a todas las áreas operativas, logísticas, administrativas y de atención al cliente de la Ferretería Multi Tableros & Herrajes S.A.

3. Marco de Referencia - ISO 31000:2018

Principios aplicados:

- Integración en los procesos de la empresa.
- Evaluación y tratamiento de riesgos asociados a las no conformidades.
- Mejora continua y toma de decisiones basada en evidencia.
- Revisión posterior y verificación de eficacia.

4. Clasificación del Riesgo Asociado a No Conformidades

Clasificación	Definición	Nivel de Riesgo	Acción Requerida
Crítica	Afecta la seguridad, continuidad operativa, o puede implicar sanciones.	**Extremo**	Acción inmediata
Mayor	Afecta significativamente los procesos o el cumplimiento interno.	**Alto**	Corrección urgente
Menor	Afectación leve, no compromete el proceso, pero representa mejora.	**Moderado o Bajo**	Mejora a corto plazo

5. Proceso de Gestión de No Conformidades

Etapa	Descripción

1. Identificación	Durante auditoría interna o inspecciones, personal detecta la NC.
2. Evaluación del Riesgo	Se clasifica el nivel de impacto de la NC según la tabla anterior.
3. Acción Correctiva	Se diseña un plan de acción proporcional al riesgo.
4. Asignación de Recursos	Se designa responsable, plazos y recursos necesarios.
5. Implementación	Se ejecuta la acción correctiva.
6. Verificación	Se realiza seguimiento para evaluar la eficacia de la corrección.
7. Registro y Cierre	Se documentan las evidencias y se cierra oficialmente la NC.

6. Tabla de Registro de No Conformidades y Acciones Correctivas

código NC	Área	Descripción de la NC	Clasificación	Evaluación de Riesgo	Acción Correctiva	Responsable	Fecha Límite	Seguimiento	Estado
NC-001	Logística	Falta de señalización de riesgo físico	Mayor	Alto	Colocar señalética en áreas críticas	Jefe de Bodega	15/07/2025	22/07/2025	Abierto
NC-002	TIC	No se realiza respaldo semanal de información	Crítica	Extremo	Programar respaldos automáticos	Jefe de Sistemas	20/07/2025	27/07/2025	Abierto
NC-003	Atención Cliente	No se registra formalmente las quejas recibidas	Menor	Bajo	Implementar bitácora digital de quejas	Supervisor Comercial	18/07/2025	25/07/2025	Abierto

7. Seguimiento y Verificación

- El área de **Gestión de Calidad o Responsable de Auditoría Interna** revisará el cumplimiento de las acciones.
- Se documentará la verificación con evidencia (fotos, reportes, respaldos, capturas de sistema, etc.).
- Si la acción no es eficaz, se reabre la no conformidad y se reajusta el plan.

8. Mejora Continua

Los resultados del proceso se analizan periódicamente para **identificar tendencias**, establecer medidas preventivas y mejorar los controles internos. Esto fortalece el sistema de gestión y reduce el riesgo general de la operación.

9. Responsables Clave

- **Gerencia General:** Revisión de cierre de no conformidades críticas.
- **Encargado de Calidad/Auditor Interno:** Seguimiento, control de plazos y archivo.
- **Responsables de Área:** Implementación de acciones correctivas.