UNIVERSIDAD PÚBLICA DE EL ALTO
VICERRECTORADO
DIRECCIÓN DE INVESTIGACIÓN CIENCIA Y TECNOLOGÍA
INSTITUTO DE INVESTIGACIONES
INGENIERÍA EN PRODUCCIÓN EMPRESARIAL

“DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO”
CASO: EMBUTIDOS COPACABANA

Resolución HCC Nº 078/2022

EQUIPO DE INVESTIGADORES:

Lic. Poly Lazaro Isaac Salazar Larico
Univ. Jesus Cristian Calle Avircata
Univ. Estefani Escurra Cabrera

EL ALTO – BOLIVIA
2022

UNIVERSIDAD PÚBLICA DE EL ALTO

AUTORIDADES

Dr. Carlos Condori Titirico
RECTOR

Dr. Efraín Chambi Vargas
VICERRECTOR

Dr. Antonio López Andrade Ph. D.
DIRECTOR DE INVESTIGACIÓN CIENCIA Y TECNOLOGÍA

Ing. Roger Llanque Villavicencio
DECANO DE ÁREA DE INGENIERÍA DE DESARROLLO TECNOLOGICO PRODUCTIVO

M.S. Ing. Ronaldo Rene Nina Tinta
DIRECTOR DE CARRERA INGENIERÍA EN PRODUCCIÓN EMPRESARIAL

ACUERDO INTERINSTITUCIONAL

Ingeniería en Producción Empresarial (IPE) – Empresa de Embutidos Copacabana

REGISTRO SENAPI: Resolución Administrativa NRO. 1-2958/2022

Dirección UPEA: Av. Sucre s/n Zona Villa Esperanza

Diciembre. 2022
El Alto – Bolivia

PRESENTACIÓN

El Instituto de Investigación de la Carrera de Ingeniería en Producción Empresarial de la Universidad Pública de El Alto como un aporte de la universidad a desarrollo científico de nuestra comunidad científica presenta el proyecto de investigación titulado “DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO” CASO: EMBUTIDOS COPACABANA”

Este proyecto de investigación consiste en desarrollar un estudio para el diseño de sistemas de seguridad electrónica para pequeñas empresas de alimentos de la ciudad de El Alto. El estudio se concentra en aplicar el proceso de gestión del riesgo que presenta la ISO 31.000 con en base el alcance, contexto y criterios para poder realizar la evaluación de los riesgos de seguridad electrónica para el resguardo físico de las instalaciones de las pequeñas empresas de alimentos y de esta manera poder identificar los riesgos, analizar, tratar los riesgos encontrados, poderlos registrar y tener un control de los mismos y de esta manera reducirlos, eliminarlos, transferirlos, o aceptarlos.

Para el Instituto de Investigación de la Carrera de Ingeniería en Producción Empresarial, el estudio pretende coadyuvar en la mejora de los mecanismos de seguridad electrónica en las instalaciones de las pequeñas empresas de alimentos de la ciudad de el Alto en los sistemas de control de accesos, alarmas, circuito cerrado de televisión y sistemas contra incendio.

M.S. Ing. Ronaldo Rene Nina Tinta
DIRECTOR DE CARRERA
INGENIERÍA EN PRODUCCIÓN EMPRESARIAL

AGRADECIMIENTOS INSTITUCIONALES

Agradecimiento a la Universidad Pública de El Alto, las autoridades y plantel administrativo, quien nos brindó la oportunidad de desarrollar el presente estudio.

Al director de Carrera de Ingeniería en Producción Empresarial del Área de Ingeniería de Desarrollo Tecnológico Productivo, por su paciencia y entrega de su tiempo para viabilizar los trámites administrativos en la Universidad.

En general a todo el equipo investigador también conformado por los estudiantes, que no su esfuerzo y empeño, logramos consolidar las partes y/o contenido del estudio.

Finalmente, a la empresa de Embutidos Copacabana por el tiempo que nos dio para realizar la presente investigación y a todas y cada una de las personas, colegas de la Universidad y amigos que me brindaron su apoyo, tiempo, ánimo e información para el logro de los objetivos.

Lic. Poly Lazaro Isaac Salazar Larico
INVESTIGADOR PRINCIPAL
INSTITUTO DE INVESTIGACIONES
INGENIERIA DE PRODUCCIÓN EMPRESARIAL

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Actualmente, en el Municipio de El Alto se concentra una gran cantidad de pequeñas empresas formales e informales en el rubro de alimentos, también podemos ver hoy en día nos encontramos en una era digital donde las herramientas tecnológicas van en constante crecimiento y las empresas y emprendimientos tiene que estar en constante aprendizaje para la mejora de ventas, producción y en esta investigación a los que viene a ser la seguridad de las instalaciones e infraestructura.

Los propietarios, dueños o gerentes de las empresas deben conocer la importancia de sus activos y de esa manera protegerla ante cualquier evento físico que puede causar corrupción de sus activos principales que puede ser la materia prima, maquinarias, productos almacenados, información de clientes, información confidencial entre otros, de esa manera al conocer una estándar para analizar los riesgos que pueden ocurrir con la empresa que es la ISO 31.000 en su versión 2018 que permitiré realizar un en un análisis de riesgo adecuado estos activos pueden identificarse para su tratamiento.

Los sistemas de seguridad electrónica permiten realizar un control y monitoreo de la infraestructura a través de la de la tecnología moderna y que principalmente se compone por los sistemas contra incendios, alarmas, circuito cerrado de televisión y control de accesos y que en base a la aplicaciones de los principios de la ISO de gestión de riesgos permite complementar el mejor aseguramiento de los riesgos con los sistemas de seguridad electrónica.

Seguidamente se elabora un diseño de sistema de seguridad electrónica sujeto a las fases y procesos que tiene la norma las cuales son el contexto, alcance, criterios, identificación de riesgos, valoración de riesgos, tratamiento, registro e informe. Y que el mismo a través de ayuda de una empresa se coloca en prueba para la verificación del diseño y que esta misma servirá para otras empresas del mismo rubro.

ABSTRACT

Currently, in the Municipality of El Alto there is a large number of small formal and informal companies in the food sector, we can also see that today we are in a digital age where technological tools are constantly growing and companies and ventures it has to be in constant learning to improve sales, production and in this investigation to what comes to be the security of the facilities and infrastructure.

The owners, owners or managers of the companies must know the importance of their assets and thus protect them against any physical event that can cause corruption of their main assets, which can be raw materials, machinery, stored products, customer information, information confidential, among others, in this way, when knowing a standard to analyze the risks that can occur with the company, which is ISO 31,000 in its 2018 version, which will allow an adequate risk analysis to be carried out, these assets can be identified for treatment.

Electronic security systems allow control and monitoring of the infrastructure through modern technology and which is mainly made up of fire systems, alarms, closed circuit television and access control and that based on the applications of the ISO risk management principles allows to complement the best insurance of risks with electronic security systems.

Next, an electronic security system design is prepared, subject to the phases and processes that the standard has, which are the context, scope, criteria, risk identification, risk assessment, treatment, registration and report. And that the same, through the help of a company, is put on trial for the verification of the design and that it will be used by other companies in the same field.

CAPITULO I: INTRODUCCION

En la actualidad toda empresa intenta basarse en la tecnología para la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento físico que puede causar corrupción de sus activos principales que puede ser la materia prima, maquinarias, productos almacenados, información de clientes, información confidencial entre otros, basándose en un análisis de riesgo adecuado estos activos pueden identificarse para su tratamiento.

Dada la importancia de la protección física, las organizaciones internacionales de estandarización han elaborado normas para la identificación, análisis, valoración y tratamiento de los riesgos que se puedas identificar para la protección de los activos.

La evolución durante las pasadas décadas que tuvo la gestión de la seguridad electrónica, así como los marcos de gobierno y gestión de riesgos, tanto corporativos como de las tecnologías de la información y las comunicaciones (TIC), hizo necesario contar con precisiones respecto del modo en que dicha gestión debiera ser llevada a cabo, a fin de asegurar el logro el cumplimiento de los objetivos de negocio.

El mejoramiento mediante estándares abarca conceptos tan globales como el planteo estratégico de la seguridad hasta cuestiones operativas. Las organizaciones, que hasta ahora han resuelto básicamente algunos problemas tecnológicos y riesgos aplicando algunas recomendaciones sobre buenas prácticas bastante generales, en este nuevo contexto intentan adecuar su gestión según alguno o varios de los estándares vigentes.

Es así como han sido desarrollados diversos estándares internacionales y regulaciones nacionales, (por ejemplo, el de la Autoridad de Supervisión del Sistema Financiero ASFI en Bolivia) que definen los principios básicos en algunos casos, y aspectos de control detallados en otros, para lograr una efectiva gestión de la seguridad Física. (ASFI, Reglamentos mínimos de seguridad, 2018).

Sin embargo, es necesario contar con algún diseño acorde a las necesidades de las empresas y con algún mecanismo que permita evaluar si los procesos involucrados resultan efectivos en

el logro de los objetivos para el que fueron diseñados para el contexto para que se pueda administrar y más aún, si facilitan la mejora continua de la gestión.

La investigación planteara un diseño de sistemas de seguridad electrónica que se sustenta en bases teóricas de la norma ISO/IEC 31000 para pequeñas empresas de alimentos de la ciudad de El Alto.

1.1 PLANTEAMIENTO DEL PROBLEMA

Los constantes hechos como ser los atracos, asaltos, en la ciudad de El Alto, esencialmente la noche directamente se vincula con la sensación de inseguridad, de la misma forma las personas extrañas o desconocidos se convierten una sensación de peligro. Los adultos identifican de peligro a los grupos de pandillas, lugares de baile, como ser las cantinas, locales de fiesta en este distrito específicos que representan la sensación de inseguridad; hay un imaginario de la inseguridad que tiende a generalizarse en la población alteña, e incluso en horas de la noche se desconfía del transporte público. La población alteña, negocios, pequeñas empresas demandan la seguridad en sus barrios mediante los radios, solicitudes escritas a las autoridades policiales tiene que ver fundamentalmente con la falta de condiciones urbanas y el deterioro físico como la ausencia o deficiente alumbrado público o espacios públicos que generan inseguridad por existir muchas discotecas, bares y lugares de diversión, las pandillas pelean y a veces asaltan a las personas a altas horas de la noche, por eso no hay seguridad. Otro elemento de importante consideración es la reapropiación de espacios públicos por grupos de jóvenes y/o adolescentes quienes consumen alcohol o drogas en plazas, jardineras, plazas, etc., son situaciones que incrementan la inseguridad en los barrios erosionando los niveles de solidaridad social y el espacio público, pues los ciudadanos toman la actitud del encierro, no salen de sus casas en algunos horarios y espacios que emiten la sensación de riesgo y el temor de ser víctima.

La ciudad de El Alto es la segunda más grande del país, motivo por el cual se generan diariamente actos de criminalidad. Actualmente la urbe alteña alberga el 76.29% de índices de inseguridad y delincuencia, llegando simplemente aun 23.71% en estadísticas de seguridad.

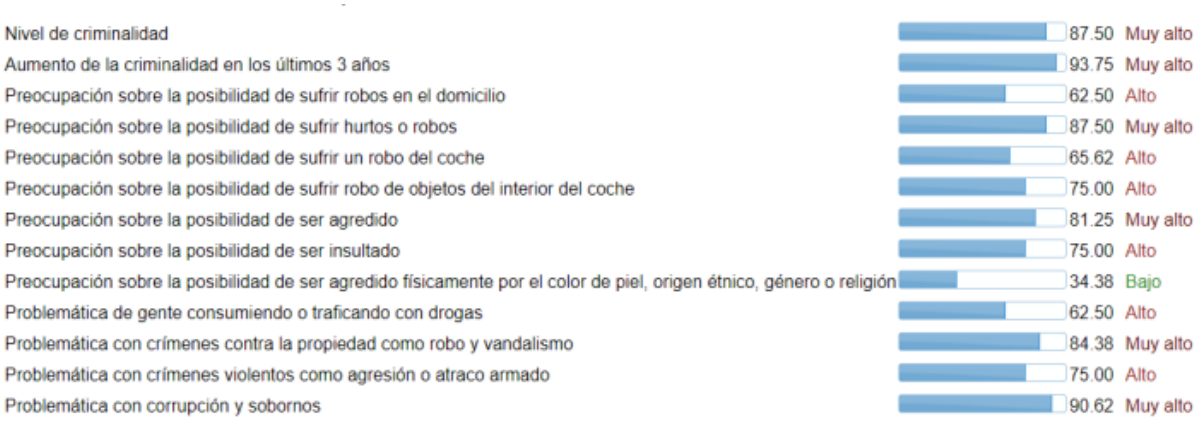


Figura 1: Tasa de criminalidad en el Alto, Periódico El Alteño 12/9/22

Dado a estudios de violencia, inseguridad y criminalidad realizado por la Oficina de Naciones Unidas contra el Delito (UNODC), la ciudad de El Alto tiene de cada 1000 casos, 27 lo cual la convierte en una de las ciudades mas inseguras y vulnerables dentro el país. Según el Observatorio Boliviano de Seguridad Ciudadana, en relación a 85 municipios de Bolivia, El Alto es donde ocurre la mayor cantidad de delitos. Los delitos y robos encabezan los hechos delictivos en la urbe alteña con un 63%. Sin embargo, bajo ciertos programas se busca reducir estos índices de criminalidad con el incremento de nuevos efectivos policiales para reforzar los patrullajes por las zonas con mayor índice de vulnerabilidad a delitos.

Por lo expuesto, se puede deducir que el principal problema en falta de seguridad, tanto como para las personas, negocios y pequeñas empresas, la falta de mejora en los sistemas en las pequeñas empresas. En tal sentido, será pertinente la aplicación del diseño de sistemas de seguridad electrónica que minimice los riesgos en las pequeñas empresas y permitan a los dueños y personas que trabajan se encuentren más seguros.

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede mitigar los riesgos físicos en las pequeñas empresas con el diseño de sistemas de seguridad electrónica?

1.3 EL OBJETIVO DE LA INVESTIGACIÓN

1.3.1 Objetivo general

Elaborar un diseño sistemas de seguridad electrónica basado en la norma ISO 31000 que minimice los riesgos en las pequeñas empresas de alimentos, caso embutidos Copacabana.

1.3.2 Objetivos Específicos

- Identificar los riesgos en los sistemas de seguridad electrónica en pequeñas empresas de alimentos.
- Analizar y valorar los riesgos identificados para su tratamiento.
- Elaborar un diseño sistemas de seguridad electrónica basado en la norma ISO 31.000 para pequeñas empresas de alimentos de la ciudad de el alto.
- Aplicar el diseño elaborado en la pequeña empresa de alimentos Embutidos Copacabana de la ciudad de El Alto.

1.4 HIPOTESIS DE LA INVESTIGACIÓN

El diseño propuesto para los sistemas de seguridad electrónica basado en la norma ISO 31000 reduce los riegos de seguridad en pequeñas empresas de alimentos la ciudad de El Alto.

1.5 JUSTIFICACIÓN DEL PROYECTO

1.5.1 Justificación Teórica

El estudio se toma como directriz fundamental en aplicar la identificación, análisis, valoración y tratamiento de los riesgos en los sistemas de seguridad electrónica basado en la norma ISO 31000 que crean y protegen el valor en las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño.

1.5.2 Justificación Metodológica

La metodología que se pretende emplear, se basara en el diseño de investigación experimental. A partir de la misma, se minimizará los riesgos de seguridad electrónica en base a la identificación de riesgos y su tratamiento basado en la norma ISO 31000 donde se identifican las variables dependientes (efectos) e independiente (causas).

1.5.3 Justificación Práctica

Con el presente estudio se propone un diseño de implementación de sistemas de seguridad electrónica para pequeñas empresas de alimentos; también coadyuvara como fuente bibliográfica o de consulta para todas aquellas pequeñas empresas que buscan aumentar su seguridad de sus instalaciones y activos principales.

1.5.4 Justificación social

Las pequeñas empresas de la ciudad de El Alto nacen siguiendo los pasos del avance de la tecnología y las mismas deben alinearse a los nuevos conceptos de seguridad donde su contexto actual de inseguridad lo exige para proteger y salvaguardar sus activos de valor y mostrar a la sociedad de la ciudad que las pequeñas empresas tiene una mejora continua y actualización constante.

CAPÍTULO II: MARCO TEÓRICO

2.1 OTROS ESTUDIOS RELACIONADOS AL TEMA

En un mundo actual de constantes cambios tecnológicos y el análisis de riesgos para el manejo de la seguridad a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado. Una efectiva administración de los riesgos asociados y su tratamiento sobre este tema es un aspecto de negocio y regulación, no sólo de tecnología.

Duvan y Ángela de la Universidad Católica de Colombia realizaron una investigación sobre los Riesgos, Amenazas y Vulnerabilidades de los Sistemas, donde determinan realizar un análisis de riesgo, donde deben tratarse técnicas de seguridad según normas ISO y la gestión de riesgos tratamiento de los riesgos para establecer controles o medidas de protección correspondientes al riesgo para proteger los activos de la organización (Castro Bolaños, Duvan Ernesto; Rojas Mora, Ángela Dayana).

Saulo Paillacho, de la Escuela Politécnica Nacional realizo una investigación de tesis de maestría que propone un Modelo de Proceso de Gestión de Riesgo de Seguridad para los activos de una organización donde inicialmente genera matrices de riesgo de los activos, valor de probabilidad, ocurrencia y riesgo para cualquier tipo de organización. El tratamiento se sustenta en un plan estratégico cumpliendo normas ISO para realizar el tratamiento del riego en sus diferentes etapas como una actualización periódica continua (Paillacho Arias, 2015).

2.2 PUNTOS DE VISTA DE OTROS INVESTIGADORES

De la misma forma se revisó los puntos de vista de otros investigadores sobre la implementación de sistemas de seguridad electrónica y los beneficios que traen sus implementaciones, de las cuales se resaltan los siguientes:

En el trabajo de grado bajo el Titulo “DESARROLLO DE UN SISTEMA DE SEGURIDAD ELECTRÓNICA APLICADO A LA SUPERVISIÓN Y MONITOREO EN OFICINAS”, Autor: Jesús Bernardo Sánchez Capistrano; donde se indican que todo ciudadano o propietario de algún inmueble requiere proteger su integridad como bienes, por ello el proyecto busca diseñar y desarrollar un sistema de seguridad electrónica basado en el control y monitoreo a través de la computadora o dispositivos conectados en red que servirá para gestionar la seguridad del local o las oficinas, que sirva como herramienta ante la presencia de hurto o intrusión, en tal

sentido en conclusión indica que los sistemas de seguridad electrónica diseñado en una empresa, ayuda a controlar la tecnología, sirviendo como control y monitoreo ante cualquier situación de inseguridad que se pudiera presentar, favoreciendo a los trabajadores y propietarios. (Sánchez Capistrano, 2019)

En la investigación de tesis de grado con título: "IMPLEMENTACIÓN DE SISTEMA DE SEGURIDAD CON VIDEO-VIGILANCIA Y SOFTWARE LIBRE" Autores: Rivas Cruz Juan Antonio y Velazquez Villa Carlos Antonio, en la cual realizan una implementación de un sistema de seguridad de video-vigilancia, capaz de realizar avisos remotos (por medio de un mensaje de correo electrónico), utilizando cámaras de distintas características y distinto fabricante, lo que le da al sistema flexibilidad para posteriores modificaciones y finalmente monitorear el área vigilada de forma remota, únicamente por medio de una contraseña y usuario determinados, desde cualquier parte del mundo por mediante la red de internet.(Rivas Cruz y Velazquez Villa, 2011)

En la investigación de tesis de grado titulado: "ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGIA MAGERIT", Autores: Antonio José Lucero Gómez John y Oswaldo Valverde Padilla, en sus conclusiones que la aplicación del modelos como MAGERIT versión 2 -Metodología de Análisis y Gestión de Riesgos permiten contribuir a que la institución posea un conocimiento claro sobre los riesgos que pueden presentarse en sus instalaciones.

2.3 MARCO REFERENCIAL

A continuación, se detalla definiciones importantes relacionadas para el desarrollo de la investigación planteada, teniendo como propósito mostrar un procedimiento coordinado y coherente de conceptos, contribuyendo de esta forma a la interpretación.

2.3.1 Riesgo

Un riesgo se refiere a la probabilidad, la estimación y la cuantificación de la magnitud y las consecuencias de los daños ambientales, sociales, económicos o culturales y/o pérdidas humanas, de bienes, etc. resultado del desencadenamiento de una amenaza. (Mauricio Chavarro, 2008)

Los riesgos se pueden estimar de acuerdo con varios factores:

- El tipo de amenaza
- El grado de exposición a dicha amenaza
- La magnitud de los daños yo perdidas
- La capacidad de repuesta en prevención; de control del fenómeno o de la amenaza, y de reducción de los daños que puede ocasionar una amenaza
- La vulnerabilidad que se tiene frente a la amenaza

RIESGO = AMENAZA X VULNERABILIDAD

2.3.1.1 Amenaza

Las amenazas son las situaciones que desencadenan en un incidente en la empresa, realizando un daño material o pérdidas inmateriales de sus activos de información. El Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 ayuda a controlar las amenazas que pueden desencadenar los incidentes. La definición de amenaza es la diversidad de consecuencias, lo que hay que tener en cuenta es examinar el impacto. Características de las amenazas la definición anterior recoge la esencia de las amenazas, es decir, es un potencial evento.

La consecuencia de las amenazas es un incidente que modifica el estado de seguridad de los activos amenazados, por lo que se hace pasar de un estado anterior al evento a otro posterior, de cualquier forma, que se trate la amenaza o las agresiones materializadas. La distancia que hay entre la amenaza potencial y su materialización como agresión real se mide por la frecuencia o la potencialidad de esta materialización, por lo que se cuenta una agresión materializada, las amenazas se verán si son agresiones potenciales o maternizadas.

2.3.1.2 Vulnerabilidad

La vulnerabilidad de un activo de seguridad es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información. La vulnerabilidad es una propiedad de la relación entre un activo y una amenaza, aunque se suele vincular más al activo como una no calidad de éste. La vulnerabilidad es un concepto que tiene dos aspectos básicos:

- Forma parte del estado de seguridad del activo en su función-propiedad de mediación entre el activo y la amenaza como acción.

- En su aspecto dinámico, es el mecanismo obligado de conversión de la amenaza en una agresión que se ha materializado sobre el activo de información

2.3.1.3 Tipos de vulnerabilidad

Se pueden considerar dos acepciones principales:

- La vulnerabilidad intrínseca del activo respecto del tipo de amenaza sólo depende de ambas cantidades.
- La vulnerabilidad efectiva del activo tiene en cuenta las salvaguardas aplicadas en cada momento a dicho activo, como un factor en el que se estima la eficacia global de dichas salvaguardas.

2.3.1.4 Atributos de las vulnerabilidades

La vulnerabilidad intrínseca puede descomponerse en análisis detallados, que se encuentran en varios bloques de atributos:

- Potencialidad autónoma respecto al activo de seguridad que se encuentre amenazado.
- Potencialidad derivada de la relación entre activo y amenaza.
- Factores subjetivos generadores de más o menos fuerza.
- Oportunidad de acceso al dominio si se tiene la suficiente capacidad y los recursos necesarios, que son cuatro: Accesibilidad física presencial, accesibilidad física cualificada, accesibilidad lógica competencial y accesibilidad lógica instrumental.

2.3.1.5 Matrices de riesgos

Una matriz de riesgos es una sencilla pero eficaz herramienta para identificar los riesgos más significativos inherentes a las actividades que desarrolla una organización, aplicable en cualquier tipo de escenario o proceso. Por lo tanto, es un instrumento válido para mejorar el control de riesgos y la seguridad corporativa.

A través de este instrumento se puede realizar un diagnóstico objetivo y global de empresas de

diferentes tamaños y sectores de actividad. Asimismo, mediante la matriz de riesgo es posible evaluar la efectividad de la gestión de los riesgos, tanto financieros como operativos y estratégicos, que están impactando en la misión de una determinada organización (Mora, 2016).

Las características que tiene las matrices de riesgo son las siguientes con el fin de garantizar su eficacia y utilidad:

- Debe ser flexible.
- Comprensible tanto al elaborar como al consultar.
- Que permita realizar un diagnóstico objetivo de la totalidad de los factores de riesgo.
- Actualizable en el tiempo entre otras.
- Desde su concepción metodológica las matrices se componen de dos vectores, uno de probabilidad y otro de impacto, cuya combinación define el nivel de riesgo de una acción en particular
- Cabe aclarar que el nivel de riesgo cero (0) no existe en la naturaleza por definición.

Una vez definidos los parámetros, los mismos permiten absorber la información de las fuentes definidas, para valorizarla en los respectivos vectores de probabilidad e impactos.

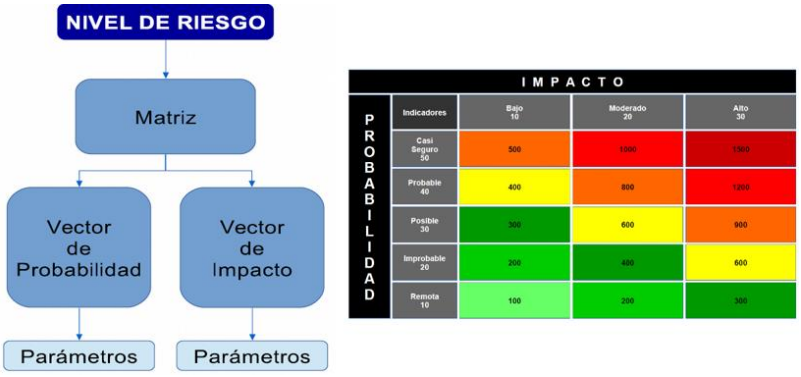


***Figura 2*:** Estructura de matriz de riesgo y ejemplo (Mora, 2016)

2.3.1.6 Estimación de riesgos

A nivel teórico existen dos posibilidades para abordar el cálculo del riesgo a partir de los valores agregados de impacto y probabilidad.

- El primero es multiplicar ambas variables (UIF de Australia 2006).

  RIESGO = PROBABILIDAD X IMPACTO

- El segundo implica establecer rangos similares para ambas y calcular el nivel de riesgo en función de la suma de las dos (Egmont, 2008).

2.3.2 Seguridad

Seguridad es el conjunto de acciones enfocadas a la protección, defensa y preservación de las personas y su entorno frente a amenazas externas que atenten contra su integridad.

De todas formas, cabe decir que la seguridad es un concepto amplísimo, aplicable a muchas situaciones y contextos, que van desde la tecnología hasta el derecho.

2.3.3 Electrónica

Finalizando la década de los cuarenta, la electrónica no tenía mayor consideración que la de ser una rama secundaria de la electricidad cuya función principal era reducir el volumen de los elementos eléctricos tradicionales; esta concepción cambia radicalmente al descubrirse el uso de los semiconductores, tales materiales permitieron la creación de dispositivos (siendo el primero el transistor) capaces de manipular la energía para el transporte de la información.

De esta manera se concibe a la electrónica de una nueva forma, como la ciencia que permite obtener, controlar y utilizar información (en forma de energía eléctrica) procedente de la naturaleza o del ser humano.

2.3.3.1 Arquitectura de un Sistema de Seguridad Electrónica

El concepto de seguridad es amplio y aplicable a un gran número de situaciones, por esta razón para alcanzar una seguridad integral es necesario utilizar medios de diversa naturaleza cuyo uso conjunto permite una mejor aproximación al bajo riesgo. La clasificación de tales medios se muestra a continuación:

- Recursos o medios humanos: Constituidos por personal capacitado de seguridad pública (Policía Nacional) o privada.
- Medios Técnicos: Todo recurso físico encaminado a mantener a la seguridad de sitios y personas, pueden ser de tipo pasivo (construcciones, vallas, etc.) o activo (dispositivos electrónicos).
- Medios Organizativos: Todas las herramientas utilizadas en la organización y coordinación en el uso de recursos, como la planificación, asignación de recursos, normas de seguridad, aplicación de los medios técnicos activos, sin embargo, a

continuación, se muestra una breve descripción de ambos tipos de medios técnicos, para tener una idea más global de un sistema de seguridad.

2.3.4 Sistemas de Seguridad electrónica

Tomando en cuenta las consideraciones anteriores podemos decir que un sistema de seguridad electrónica será la interconexión de recursos, redes y dispositivos (Medios técnicos activos) cuyo objetivo es precautelar la integridad de las personas y su entorno previniéndolas de peligros y presiones externas.

El uso de estos recursos, dependerá (como ya se dijo) de la características y necesidades de aquello que se va a proteger, considerándose el número de sitios a proteger, los riesgos potenciales de los mismos y necesidades especiales que se puedan presentar.

Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, bóvedas, áreas de exclusión, rack de telecomunicaciones, etc.), la vigilancia óptica mediante fotografía o circuito cerrado de televisión (CCTV) y la intercomunicación por megafonía y protección de las comunicaciones.

Figura 3: Sistemas de Seguridad Electrónica (Roca Chillida, 2017)

2.3.5 Sistemas de intrusión

La tecnología relacionada con la detección de intrusos dispone de sistemas inalámbricos, teclados y dispositivos de mando remoto, centrales de alarmas, sistemas de comunicación y

programación, sistemas de detección perimetral, barreras y sensores infrarrojos, sirenas para interior o exterior, etc. Así, se convierte en un elemento fundamental que permite detener a individuos sospechosos antes de cometer sus delitos, haciendo que el servicio de la empresa de seguridad privada sea más eficaz y solvente (Roca Chillida, 2018).

Se detalla algunos dispositivos de seguridad que son utilizados en dicho sistema los cuales son:

- Sensores de movimiento
- Detectores de humedad
- Detectores de temperatura
- Detectores de agua
- Detectores de gases
- Sensores de vibración
- Sensores de golpe
- Contactos magnéticos
- Sensores de ruptura de vidrios
- Sensores antifraude
- Pulsadores de pánico
- Sirenas
- Llaves Shunt

Cabe destacar que la seguridad electrónica también es compatible con los sistemas de detección de incendios mediante la instalación de sensores y accesorios que pueden ser inalámbricos o cableados, equipos homologados con la normativa legal vigente, sirenas y pulsadores, dispositivos de emergencia, entre otros.

Figura 4: Dispositivos de Seguridad Electrónica (Roca Chillida, 2017)

2.3.6 Sistemas de control de accesos

La seguridad electrónica también ofrece importantes recursos en el control de accesos a través de la instalación de monitores. Con ellos puede controlarse el flujo de personas, vehículos y cualquier tipo de activo en un ámbito determinado o en diferentes localizaciones de la misma empresa. Habitualmente cuenta con tecnologías de control, tanto para fábricas como para edificios, sistemas de tarjeta de proximidad y de lectura, control inalámbrico, sistemas biométricos de reconocimiento facial o por huella digital, integración con redes IP, cerraduras electromagnéticas, etc.

2.3.7 Sistemas de circuito cerrado de televisión

CCTV (Circuito Cerrado de Televisión) una herramienta esencial dentro del sistema de control y vigilancia para las empresas, que cuenta con cámaras, tanto para el interior como para el exterior-, Domos y controladores, grabadoras digitales DVR/NVR, equipos PCI, tecnología coaxial e IP, etc.

Un apartado fundamental de la tecnología de seguridad electrónica es la capacidad de visualizar las cámaras desde la oficina o a través de la red desde cualquier punto y a cualquier hora. Es clave para la tranquilidad en el entorno laboral. (Jordi Gutiérrez, 2016)

2.3.8 Norma ISO 31000

Es una norma internacional tiene el objetivo de ayudar a las organizaciones de todo tipo y tamaño a gestionar el riesgo con eficiencia.

La norma ISO 31000 se puede aplicar a cualquier tipo de riesgo, no importa cuál sea su naturaleza, su origen, su causa o que sus consecuencias sean positivas o negativas para la empresa. El estándar establece los principios, el marco de trabajo y el proceso que se debe seguir para gestionar cualquier tipo de riesgo de una forma transparente, sistemática y creíble dentro de cualquier contexto.

2.3.8.1 Directrices genéricas para la gestión de riesgos

La norma ISO 31000 establece todos los principios y directrices de carácter genérico sobre la gestión del riesgo.

Para establecer una mayor eficiencia, la gestión del riesgo en una empresa tiene que contar con los siguientes principios básicos:

- Incrementar la probabilidad de conseguir los objetivos
- Motivar a la dirección de forma proactiva
- Ser consciente de lo necesario que es identificar y tratar el riesgo en todas las partes de la empresa
- Mejorar la identificación de las oportunidades y las amenazas
- Cumplir con las exigencias legales y los requisitos de regulación, además de con las normas internacionales
- Mejora la gobernabilidad dentro de la organización
- Mejora la confidencialidad y confianza de las partes interesadas
- Establece una base confiable para la toma de decisiones y la planificación
- Mejora los controles
- Asigna con eficacia la utilización de los recursos para el **tratamiento del riesgo**
- Mejora la eficiencia y la eficacia de las operaciones que realiza la organización.
- Mejora la prevención contra las pérdidas
- Mejora el manejo de los incidentes

- Disminuye las pérdidas
- Mejora el conocimiento de la empresa
- Mejora la capacidad de recuperación de la empresa

2.3.8.2 Principios básicos para la gestión de riesgos

- Tiene que ser integrado y no aislado del resto de procesos de la organización.
- El SG va a ser estructurado, es decir, tiene que presentar resultados consistentes, que permitan comparar de manera tangible un periodo con otro, y observar el avance.
- Ser adaptable, de manera que se ajuste al contexto organizacional y esté íntimamente relacionado con los objetivos.
- Debe ser inclusivo e involucrar a cada una de las partes interesadas a tener en cuenta, para conseguir una gestión de riesgos más informada.
- Dinámico y que responda a los cambios o se anticipe a ellos.
- Basado en la mejor información disponible, respetando la confidencialidad a todos los niveles, especialmente, las partes interesadas.
- Considerar los factores humanos y culturales que les influyen, tanto interna como externamente.
- Mejora continua, a través del aprendizaje que da la experiencia.

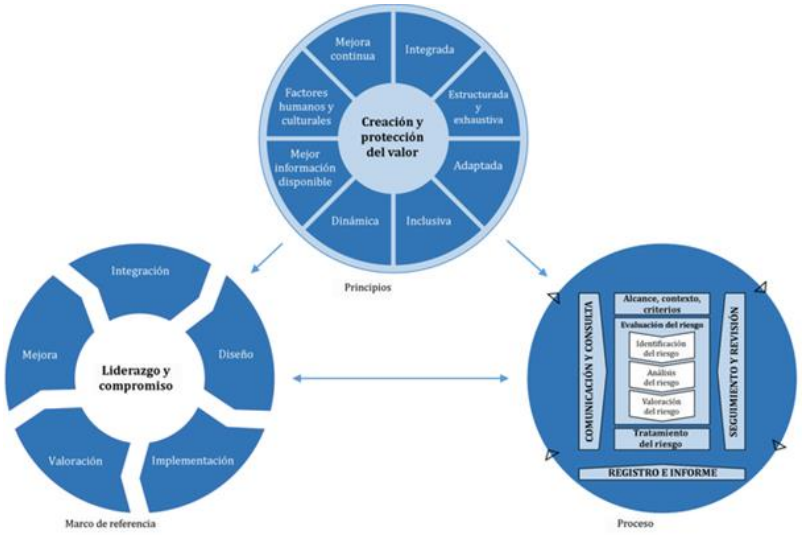


Figura 5: Directrices de gestión de riesgos (ISO 31.000:2018)

2.3.8.3 Tratamiento del riesgo

El objetivo del tratamiento de riesgos según ISO 31000:2018 es diseñar, evaluar, seleccionar e implementar acciones para abordar los riesgos identificados dentro de una organización.

El tratamiento de riesgos según ISO 31000:2018 es un proceso dinámico e iterativo que requiere:

- Formular opciones para el tratamiento de riesgo.
- Seleccionar la opción más adecuada.
- Planificar e implementar el tratamiento de riesgos.
- Evaluar la efectividad de las acciones implementadas.
- Calificar el riesgo residual (aceptable o no aceptable).
- Tratamiento para el riesgo residual no aceptable.

La selección de las opciones de tratamiento de riesgo que resulten más efectivas, requiere poner en una balanza los beneficios potenciales derivados de la efectividad de la acción propuesta, por un lado, y el coste, el esfuerzo y las desventajas que eventualmente pudiesen surgir como consecuencia de la implementación.

Las opciones de tratamiento de riesgos según ISO 31000:2018 no son excluyentes entre sí. Tampoco resultan eficaces en todas las circunstancias. Éstas pueden incluir una o varias de las siguientes acciones:

- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
- Asumir el riesgo, aun aumentándolo, con el fin de incrementar una posible oportunidad.
- Tomar acciones para disminuir la probabilidad del riesgo.
- Implementar acciones que disminuyan el impacto negativo del riesgo.
- Compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros)
- Retener el riesgo con base en información confiable.

La razón para implementar planes de tratamiento de riesgos es definir y especificar la forma en que se adoptarán las opciones elegidas, para que todas las partes interesadas las entiendan y sea posible monitorear el progreso del plan.

El plan de tratamiento de riesgos según ISO 31000:2018 debe identificar con claridad el orden en que se deben implementar las acciones, y la forma en que se integrará con los procesos de gestión de la organización, todo ello de acuerdo con las necesidades de las partes interesadas.

La información provista en el plan de tratamiento de riesgos debe incluir:

- Justificación para la elección de las opciones de tratamiento, incluyendo beneficios esperados.
- Quiénes son los responsables de aprobar e implementar el plan.
- Las acciones de tratamiento propuestas.
- Recursos requeridos, incluyendo los necesarios en caso de contingencia.
- Mediciones de rendimiento del plan.
- Limitaciones del plan.
- Acciones de monitoreo requeridas.
- Plazos esperados para que se completen las acciones.

2.4 ENFOQUE ELEGIDO POR EL INVESTIGADOR

Efectuado los análisis de las investigaciones referidos al tema, será importante aplicar las herramientas de gestión de riesgo para que permita enfocar ciertas amenazas y vulnerabilidades que se tiene en pequeñas empresas de alimentos en la ciudad de El Alto, con un enfoque cuantitativo tomando en cuenta los sistemas de seguridad electrónica como ser: sistema contra incendio, sistema de alarmas, circuito cerrado de televisión y sistema de control de acceso permiten el aseguramiento físico de las empresas.

En nuestra actualidad en la ciudad de El Alto el índice de delincuencia que va creciendo y se tiene que tomar aspectos de aseguramiento adecuados para la empresa en ese sentido los dispositivos que componen los sistemas de seguridad electrónica son gran una ayuda esencial, estas instalaciones se las debe trabajar con un criterio que ayude a la empresa a

darle una adecuada solución y por tal motivo en la presente investigación se elige a la herramienta de consulta del estándar de la ISO 31.000:2018 el cual es una herramienta que permite en primer lugar definir ciertos criterios de contexto, alcance, coordinación, evaluación de los riesgos, así como su proceso de identificación, análisis, evaluación y tratamiento es posible tener indicadores que ayude a mejorar los mecanismos de seguridad e implementar los controles, sistemas, responsables y categorización a medida de una empresa.

Actualmente muchas empresas no cuentan con sistemas de seguridad electrónica para la protección de sus instalaciones en las áreas importantes el presente proyecto pretende aportar con un diseño en base a la experiencia que se tiene con la empresa de embutidos Copacabana para otras empresas puedan instalar estos sistemas de acuerdo a sus necesidades en base a la recolección de información dado por la ISO 31.000:2018.

2.5 IDENTIFICACIÓN DE FUENTES

2.5.1 Fuentes primarias

La información primaria se obtuvo en base a la investigaciones similares realizadas donde podemos apreciar la aplicabilidad de las herramientas y metodologías para el tratamiento de riesgos entre los cuales se puede mencionar de la Universidad Católica de Colombia realizaron una investigación sobre los Riesgos, Amenazas y Vulnerabilidades de los Sistemas, donde determinan realizar un análisis de riesgo, donde deben tratarse técnicas de seguridad según normas ISO y la gestión de riesgos tratamiento de los riesgos para establecer controles o medidas de protección correspondientes al riesgo para proteger los activos de la organización (Castro Bolaños, Duvan Ernesto; Rojas Mora, Ángela Dayana), asimismo la investigación de la Escuela Politécnica Nacional realizo una investigación de tesis de maestría que propone un Modelo de Proceso de Gestión de Riesgo de Seguridad para los activos de una organización donde inicialmente genera matrices de riesgo de los activos, valor de probabilidad, ocurrencia y riesgo para cualquier tipo de organización. (Paillacho Arias, 2015).

2.5.2 Fuentes secundarias

La información secundaria es obtenida a través de estudios relacionados a los sistemas de seguridad electrónica como el estudio de “Desarrollo de un sistema de seguridad electrónica aplicado a la supervisión y monitoreo en oficinas”, Autor: Jesús Bernardo Sánchez Capistrano; donde se indican que todo ciudadano o propietario de algún inmueble requiere proteger su

integridad como bienes, por ello el proyecto busca diseñar y desarrollar un sistema de seguridad electrónica basado en el control y monitoreo a través de la computadora o dispositivos conectados en red (Sánchez Capistrano, 2019) así mismo la investigación de tesis de grado con título: “Implementación de sistema de seguridad con video-vigilancia y software libre” Autores: Rivas Cruz Juan Antonio y Velazquez Villa Carlos Antonio, en la cual realizan una implementación de un sistema de seguridad de video-vigilancia, capaz de realizar avisos remotos (por medio de un mensaje de correo electrónico), (Rivas Cruz y Velazquez Villa, 2011).

Libros

En el libro “Los alcances de la seguridad e importancia de gestión de riesgo en nuestro enfoque de seguridad” elaborado por Fernando Angel Quiroga Pastrana, donde indica que la seguridad y la prevención son conceptos indivisibles para lograr un clima de estabilidad física y emocional, sin embargo, la continuidad y el fortalecimiento del verdadero significado de estas categorías son en definitiva una prioridad.

En el libro de “Certificación internacional para operadores de consola de CC.TV. y medios tecnológicos de seguridad”, de la Escuela Latinoamericana de Seguridad ESLASEG – INTERNACIONAL, donde se puede apreciar medios de protección físicos y tecnológicos.

Al mismo tiempo se obtuvo información adicional en bibliotecas virtuales de universidades, páginas web, ministerios e instituciones especializadas en investigación.

CAPÍTULO III: MARCO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Para el desarrollo del Diseño de Sistemas de Seguridad Electrónica Basado en la norma ISO 31.000 para pequeñas empresas de alimentos de la ciudad de El Alto se utilizó el estudio de investigación tipo "Exploratorio" porque se identificaron las relaciones entre factores que nos permitieron determinar tendencias, consecuencias, daños, vulnerabilidades, entre otros. También se utilizó el estudio de investigación tipo “Descriptivo” porque se nos permitió interpretar los resultados del modelo propuesto. Finalmente se utilizó el tipo de investigación tipo “Correlacional” porque permitió describir e interpretar las relaciones entre variables en base al análisis de información generada.

3.2 DISEÑO DE LA INVESTIGACIÓN

El diseño metodológico que se utilizó en la investigación para llegar a los objetivos maximizando la información y reduciendo errores en los resultados fue el diseño de investigación en experimental, como su nombre lo indica es una situación de control, en la cual se manipulan de manera intencional, una o más variables independientes (causas), para analizar las consecuencias de tal manipulación sobre una o más variables dependientes (efectos). Este diseño metodológico permitió que la investigación analizar el grado de contribución para el Diseño de Sistemas de Seguridad Electrónica Basado en la norma ISO 31.000 (variable independiente) riesgos en pequeñas empresas de alimentos de la ciudad de el alto, Caso: Embutidos Copacabana (variable dependiente)

También se utilizó el método hipotético-deductivo, que permitió observar el campo de investigación, formular una hipótesis, deducir consecuencias e implicaciones más elementales de la propia hipótesis y comprobar enunciados deducidos comparándolos con la experiencia realizada durante el desarrollo y conclusión de la investigación.

3.3 VARIABLES DE LA INVESTIGACIÓN

Son las características y propiedades cuantitativas o cualitativas de un objeto o fenómeno que adquieren distintos valores y varían respecto a las unidades de observación.

Tabla 1: Identificación de variables

Variable dependiente	Variable Independiente
Riesgos en pequeñas empresas de alimentos de la ciudad de el alto, Caso: Embutidos Copacabana	Diseño de Sistemas de Seguridad Electrónica Basado en la norma ISO 31.000

Fuente: Elaboración propia

3.3.1 Operacionalización de variables

Tabla 2: Operacionalización de variable dependiente

Nombre	Definición conceptual	Componentes	Dimensión	Indicadores
Riesgos en Pequeñas empresas de alimentos de la ciudad de el alto, Caso: Embutidos Copacabana	Es la Probabilidad de que se produzca un contratiempo o desastre en los sistemas de seguridad electrónica	Amenazas y riesgos en los sistemas de seguridad electrónica Vulnerabilidades internas Impacto	Eventos que puedas ocasionar daño Falta de seguridad, de confianza o de certeza sobre algo, especialmente cuando crea inquietud Es el resultado, la consecuencia, lo que se deriva de una causa	Nro. de amenazas y riesgos identificados Nro. de vulnerabilidades identificadas Materialización monetaria del impacto

Fuente: Elaboración Propia

Tabla 3: Operacionalización de variable independiente

Nombre	Definición conceptual	Componentes	Dimensión	Indicadores
Diseño de Sistemas de Seguridad Electrónica Basado en la	Aplicación de barreras, procedimientos de control, como medidas	Análisis de riesgos Valoración de los riesgos	Establecimiento de probabilidad e impacto en los riesgos identificados	Nro. de riesgos evaluados y calificados

norma ISO 31.000	de prevención y contramedidas ante los riesgos de los sistemas de seguridad electrónica basados en las buenas prácticas de la ISO 31000	Políticas de administración de riesgos Monitoreo y revisión	Establecimiento de medidas de mitigación Tratamiento de riesgos en base al apetito de riesgo Seguimiento sobre las medidas que se establecen para la gestión de riesgos	Nro. de controles de mitigación elaborados Nro. de riesgos aceptados, trasferidos, eliminados y mitigados

Fuente: Elaboración Propia

3.4 POBLACIÓN Y MUESTRA

En el caso de la presente investigación al tratarse del diseño de sistemas de seguridad electrónica basado en la norma ISO 31.000 y el mismo es aplicado en la empresa de Embutidos Copacabana no amerita población y muestra, en el sentido de que el diseño del sistema de seguridad electrónica será elaborado para todos los ambientes físicos de la empresa.

3.5 AMBIENTE DE LA INVESTIGACIÓN

El presente estudio se realizará en el Municipio de El Alto, en coordinación con la pequeña empresa de embutidos Copacabana y en las oficinas del Instituto de Investigaciones de la carrera de Ingeniería en Producción Empresarial.

Para fines comparativos, se pretenderá realizar estudios de procesos productivos, consideradas como automatizadas, semiautomatizadas y manuales.

3.6 TÉCNICAS E INSTRUMENTOS

A continuación, se detallan las técnicas e instrumentos aplicados en el presente trabajo de investigación:

- Entrevistas: A los encargados de pequeñas empresas de alimentos que permitirá obtener información de vulnerabilidades y amenazas en los Sistemas de Seguridad Electrónica, obteniendo información de la empresa, viendo el contexto, ubicación, áreas de trabajo, personal administrativo, horarios de trabajo, controles existentes, cantidad de sistemas de seguridad en funcionamiento e información adicional.
- Consultas: A funcionarios que interactúan con los manejos de activos importantes en la empresa de alimentos, que permita realizar una clasificación de la información entre lo sistemas de seguridad electrónica, elaborando un análisis de los riesgos adecuado y a medida de la empresa que permite el aseguramiento de los ambientes y áreas de acuerdo a la criticidad y valor de los activos.
- Observaciones: Con visitas a la empresa realizando recolección de información fotografías de todos los ambientes, manejo de los sistemas de seguridad contra incendios, monitoreo a través de circuito cerrado de televisión, controles de acceso y sistema de alarmas de intrusión.
- Revisión de documentación: Obtener información que ayude a con la investigación, como reglamentos existentes, controles, manual de funciones de los trabajadores, que permite realizar identificar controles de los sistemas, y la responsabilidad de monitoreo y seguimiento en los sistemas de seguridad electrónica, así también permitirá elaborar y determinar el tratamiento de riesgo identificado y valorado.

3.7 PROCEDIMIENTO DE LA INVESTIGACIÓN

El siguiente cuadro nos da a conocer las fases que se realizó en la investigación mediante las metodologías utilizadas.

Tabla 4: Fases del procedimiento de investigación

Nro.	Descripción
FASE 1:	Recolección de información de comunicación y consulta

FASE 2: Definición de alcance, contexto y criterios

FASE 3: Evaluación del riesgo

FASE 4: Identificación del riesgo

FASE 5: Análisis del riesgo

FASE 6: Valoración del riesgo

FASE 7: Tratamiento del riesgo

FASE 8: Registro e informe

Fuente: Elaboración propia

3.7.1 Fase 1: Recolección de información de comunicación y consulta

El propósito de la comunicación y consulta para la recolección de información es asistir a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. Una coordinación cercana entre ambas debería facilitar un intercambio de información basado en hechos, oportuno, pertinente, exacto y comprensible, teniendo en cuenta la confidencialidad e integridad de la información, así como el derecho a la privacidad de las personas.

La comunicación y consulta con las partes interesadas apropiadas, externas e internas, se debería realizar en todas y cada una de las etapas del proceso de la gestión del riesgo.

La comunicación y consulta pretende:

— reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del riesgo;
— asegurar que se consideren de manera apropiada los diferentes puntos de vista cuando se definen los criterios del riesgo y cuando se valoran los riesgos;

— proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones;
— construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.

3.7.2 Fase 2: Definición de alcance, contexto y criterios

3.7.2.1 Alcance

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican definir el alcance del proceso, y comprender los contextos externo e interno.

La organización debería definir el alcance de sus actividades de gestión del riesgo.

Como el proceso de la gestión del riesgo puede aplicarse a niveles distintos (por ejemplo: estratégico, operacional, de programa, de proyecto u otras actividades), es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su alineamiento con los objetivos de la organización.

En la planificación del enfoque se incluyen las siguientes consideraciones:

— los objetivos y las decisiones que se necesitan tomar;
— los resultados esperados de las etapas a ejecutar en el proceso;
— el tiempo, la ubicación, las inclusiones y las exclusiones especificas;
— las herramientas y las técnicas apropiadas de evaluación del riesgo;
— los recursos requeridos, responsabilidades y registros a conservar;
— las relaciones con otros proyectos, procesos y actividades.

3.7.2.2 Contexto

Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos.

El contexto del proceso de la gestión del riesgo se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización y debería reflejar el entorno específico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo.

La comprensión del contexto es importante porque:

- la gestión del riesgo tiene lugar en el contexto de los objetivos y las actividades de la organización;
- los factores organizacionales pueden ser una fuente de riesgo;
- el propósito y alcance del proceso de la gestión del riesgo puede estar interrelacionado con los objetivos de la organización como un todo;

La organización debería establecer los contextos externo e interno del proceso de la gestión del riesgo considerando los factores mencionados.

3.7.2.3 Definición de los criterios del riesgo

La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos. También debería definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones. Los criterios del riesgo se deberían alinear con el marco de referencia de la gestión del riesgo y adaptar al propósito y al alcance específicos de la actividad considerada. Los criterios del riesgo deberían reflejar los valores, objetivos y recursos de la organización y ser coherentes con las políticas y declaraciones acerca de la gestión del riesgo. Los criterios se deberían definir teniendo en consideración las obligaciones de la organización y los puntos de vista de sus partes interesadas.

Aunque los criterios del riesgo se deberían establecer al principio del proceso de la evaluación del riesgo, éstos son dinámicos, y deberían revisarse continuamente y si fuese necesario, modificarse.

Para establecer los criterios del riesgo, se debería considerar lo siguiente:

- la naturaleza y los tipos de las incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles);
- cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad;
- los factores relacionados con el tiempo;
- la coherencia en el uso de las mediciones;
- cómo se va a determinar el nivel de riesgo;
- cómo se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos;
- la capacidad de la organización.

3.7.3 FASE 3: Evaluación del riesgo

La evaluación del riesgo es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo.

La evaluación del riesgo se debería llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas. Se debería utilizar la mejor información disponible, complementada por investigación adicional, si fuese necesario.

3.7.4 FASE 4: Identificación del riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

La organización puede utilizar un rango de técnicas para identificar incertidumbres que pueden afectar a uno o varios objetivos. Se deberían considerar los factores siguientes y la relación entre estos factores:

- las fuentes de riesgo tangibles e intangibles;
- las causas y los eventos,
- las amenazas y las oportunidades;
- las vulnerabilidades y las capacidades;

- los cambios en los contextos externo e interno;
- los indicadores de riesgos emergentes;
- la naturaleza y el valor de los activos y los recursos;
- las consecuencias y sus impactos en los objetivos;
- las limitaciones de conocimiento y la confiabilidad de la información;
- los factores relacionados con el tiempo;
- los sesgos, los supuestos y las creencias de las personas involucradas.

La organización debería identificar los riesgos, tanto si sus fuentes están o no bajo su control. Se debería considerar que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.

3.7.5 FASE 5: Análisis del riesgo

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos.

El análisis del riesgo se puede realizar con diferentes grados de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles. Las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de éstas, dependiendo de las circunstancias y del uso previsto.

El análisis del riesgo debería considerar factores tales como:

- la probabilidad de los eventos y de las consecuencias;
- la naturaleza y la magnitud de las consecuencias;
- la complejidad y la interconexión;
- los factores relacionados con el tiempo y la volatilidad;
- la eficacia de los controles existentes;
- los niveles de sensibilidad y de confianza.

El análisis del riesgo puede estar influenciado por cualquier divergencia de opiniones, sesgos, percepciones del riesgo y juicios. Las influencias adicionales son la calidad de la información utilizada, los supuestos y las exclusiones establecidos, cualquier limitación de las técnicas y cómo se ejecutan éstas. Estas influencias se deberían considerar, documentar y comunicar a las personas que toman decisiones.

Los eventos de alta incertidumbre pueden ser difíciles de cuantificar. Esto puede ser una cuestión importante cuando se analizan eventos con consecuencias severas. En tales casos, el uso de una combinación de técnicas generalmente proporciona una visión más amplia.

El análisis del riesgo proporciona una entrada para la valoración del riesgo, para las decisiones sobre la manera de tratar los riesgos y si es necesario hacerlo y sobre la estrategia y los métodos más apropiados de tratamiento del riesgo. Los resultados proporcionan un entendimiento profundo para tomar decisiones, cuando se está eligiendo entre distintas alternativas, y las opciones implican diferentes tipos y niveles de riesgo.

3.7.6 FASE 6: Valoración del riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

— no hacer nada más;
— considerar opciones para el tratamiento del riesgo;
— realizar un análisis adicional para comprender mejor el riesgo;
— mantener los controles existentes;
— reconsiderar los objetivos.

Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.

Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

3.7.7 FASE 7: Tratamiento del riesgo

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo.

El tratamiento del riesgo implica un proceso iterativo de:

- formular y seleccionar opciones para el tratamiento del riesgo;
- planificar e implementar el tratamiento del riesgo;
- evaluar la eficacia de ese tratamiento;
- decidir si el riesgo residual es aceptable;
- si no es aceptable, efectuar tratamiento adicional.

3.7.7.1 Selección de las opciones para el tratamiento del riesgo

La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación.

Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

- evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;
- aceptar o aumentar el riesgo en busca de una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad;
- modificar las consecuencias;
- compartir el riesgo (por ejemplo: a través de contratos, compra de seguros);
- retener el riesgo con base en una decisión informada.

La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería tener en cuenta todas las obligaciones de la organización, los compromisos voluntarios y los puntos de vista de las partes interesadas. La selección de las

opciones para el tratamiento del riesgo debería realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

Al seleccionar opciones para el tratamiento del riesgo, la organización debería considerar los valores, las percepciones, el involucrar potencialmente a las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas. A igual eficacia, algunas partes interesadas pueden aceptar mejor que otras los diferentes tratamientos del riesgo.

Los tratamientos del riesgo, a pesar de un cuidadoso diseño e implementación, pueden no producir los resultados esperados y puede producir consecuencias no previstas. El seguimiento y la revisión necesitan ser parte integral de la implementación del tratamiento del riesgo para asegurar que las distintas maneras del tratamiento sean y permanezcan eficaces.

El tratamiento del riesgo a su vez puede introducir nuevos riesgos que necesiten gestionarse.

Si no hay opciones disponibles para el tratamiento o si las opciones para el tratamiento no modifican suficientemente el riesgo, éste se debería registrar y mantener en continua revisión.

Las personas que toman decisiones y otras partes interesadas deberían ser conscientes de la naturaleza y el nivel del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y ser objeto de seguimiento, revisión y, cuando sea apropiado, de tratamiento adicional.

3.7.7.2 Preparación e implementación de los planes de tratamiento del riesgo

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

Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas.

La información proporcionada en el plan del tratamiento debería incluir:

- el fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados;
- las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan;
- las acciones propuestas;
- los recursos necesarios, incluyendo las contingencias;
- las medidas del desempeño;
- las restricciones;
- los informes y seguimiento requeridos;
- los plazos previstos para la realización y la finalización de las acciones.

3.7.7.3 Seguimiento y revisión

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

El seguimiento y la revisión deberían tener lugar en todas etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

Los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

3.7.8 FASE 8: Registro e informe

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:

- comunicar las actividades de la gestión del riesgo y sus resultados a lo largo de la organización;
- proporcionar información para la toma de decisiones;
- mejorar las actividades de la gestión del riesgo;

— asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

Las decisiones con respecto a la creación, conservación y tratamiento de la información documentada deberían tener en cuenta, pero no limitarse a su uso, la sensibilidad de la información y los contextos externo e interno.

El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades. Los factores a considerar en el informe incluyen, pero no se limitan a:

— las diferentes partes interesadas, sus necesidades y requisitos específicos de información;
— el costo, la frecuencia y los tiempos del informe;
— el método del informe;
— la pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.

Difusión de los resultados

Para la difusión de resultados se realizarán talleres de capacitación en manejo de los sistemas de seguridad electrónica, como ser los sistemas de circuito cerrado de televisión, control de accesos, sistemas contra incendios, sistema de alarmas, y los dispositivos que están contentados.

CAPÍTULO IV: RESULTADOS

Considerando los objetivos del estudio y los análisis previos, a continuación, se presenta los resultados en base de la recolección de información según la norma ISO 31.000 y el contexto de abstracción de información.

4.1 Definición Alcance, contexto y criterios

4.1.1 Alcance

Como alcance de investigación dentro lo relacionado con la identificación, análisis, valoración y tratamiento de los riesgos en los sistemas de seguridad electrónica los cuales son:

- Sistemas de intrusión
- Sistemas de control de accesos
- Sistemas de circuito cerrado de televisión
- Sistema contra incendio

Los sistemas de seguridad electrónica resguardan la parte física y activos importantes de la empresa como productos, almacenes, infraestructura, maquinaria, entre otros.

4.1.2 Contexto

La empresa de embutidos “COPACABANA”, se encuentra ubicada en la ciudad de El Alto, Distrito Municipal 5, Urb. German Busch, calle Puerto Belén N° 2035.

Figura 6: Ubicación de la empresa

4.1.2.1 Organización de la Empresa

La empresa de embutidos COPACABANA cuenta con tres áreas administrativas divididas de la siguiente manera:

- **Departamento de Contabilidad**. - está conformado por dos personas que están encargadas del manejo: de las cuentas de activo, pasivo y patrimonio, de las transacciones diarias, registros, informes financieros y control al cumplimiento con las políticas establecidas por el sector público.
- **Departamento de Producción. -** está conformado por un equipo de personal quienes se encargan de la elaboración de la diversidad de productos con el cumplimiento de las respectivas normas de calidad e higiene, además cuentan con un jefe de producción el cual tiene la responsabilidad de dirigir y controlar que el producto sea óptimo para la máxima satisfacción de los clientes.
- **Departamento de Ventas**. - está conformado por dos personas que están encargadas de realizar las ventas al público en general, de informar a los clientes sobre los diferentes productos que la empresa ofrece, los descuentos, promociones y formas de pago.

4.1.2.2 Descripción técnica de la empresa

Materia prima, insumos, materiales

La materia prima se constituye en la adquisición de la carne de chancho.

Productos

Los productos de la unidad industrial, Embutidora “COPACABANA” son:

- Queso de chancho
- Mortadela
- Salchicha

Descripción de las operaciones del proceso productivo

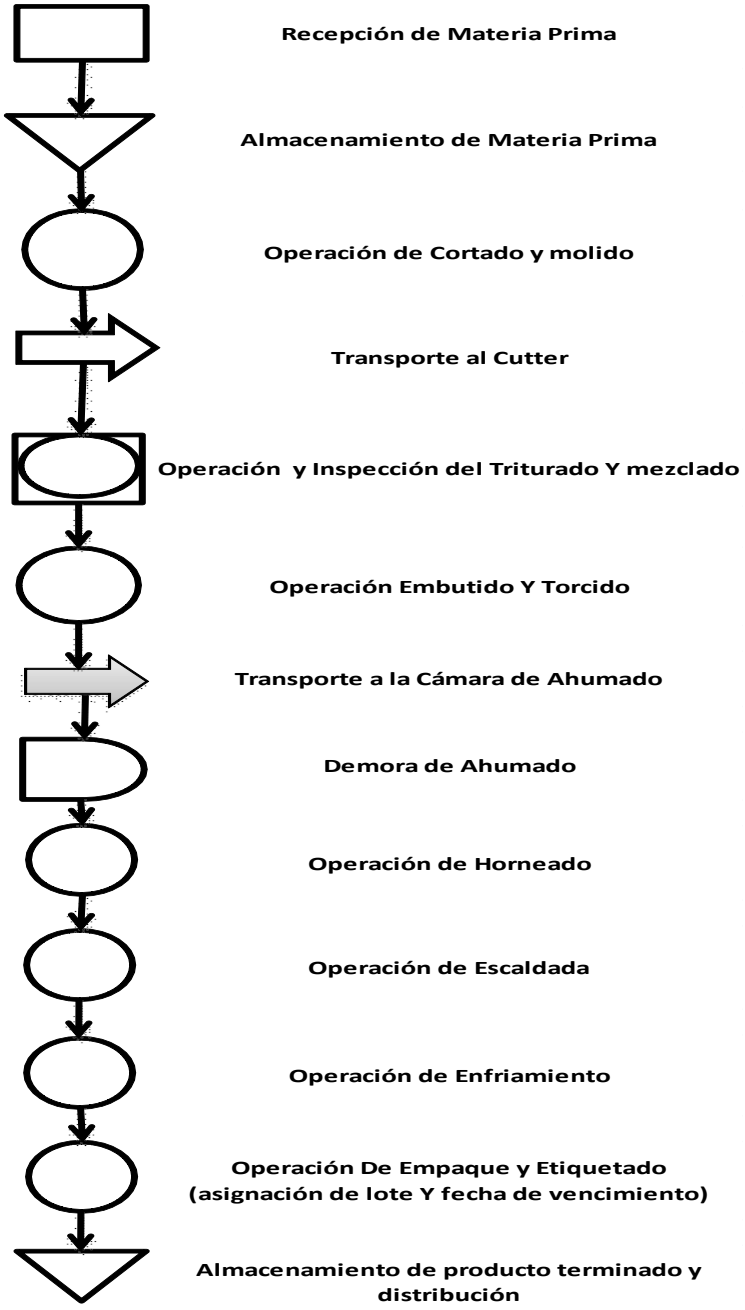


Figura 7: Diagrama de flujo de proceso de elaboración de salchichas

Elaboración de salchichas

Las salchichas es un embutido escaldado elaborado en base a carne de res y carne de cerdo, grasa, especias, sal, emulsificantes, aglutinantes y otros aditivos de uso permitido. La masa, después de procesada, se embute en tripas artificiales o naturales, se somete a cocción y

eventualmente se ahúma. Se presentan como salchichas de 12 a 15cm de largo y un diámetro de 12 a 25mm.

Proceso de elaboración

Troceado y Curación Preliminar

Las carnes se cortan en piezas de 5 a8cm, se les añade la mezcla de curación, la sal y el azúcar, dispersando todo en forma homogénea. La mezcla se deja en la cámara de curado o en refrigeración durante 24 horas.

Molido y Picado

Después de as 24 horas, se sacan del refrigerador los trozos de carne y se muelen pasándolos por el disco de agujeros de 3mm. La grasa también se muele pasándola por el mismo disco.

Emulsificante (cutter)

La carne ya molida se coloca en la cutter se añade la mitad de los polifosfatos; con la máquina operando se adiciona gradualmente el hielo picado, se adiciona también el polifostato restante, luego se añaden las especias y la cebolla molida. Cuando los ingredientes añadidos se hayan bien integrados, se añade la grasa molida, se pica por 3min y se agrega el emulsificante, continuando la operación por 3min más. El tiempo total del picado no debe pasar de los 12min; la temperatura de la masa debe ser menor de 15ºC. Al final la mezcla debe quedar finamente molida y su apariencia debe ser homogénea.

Embutido

La masa se embute en tripas artificiales de 1,5 a 2cm de diámetro; se debe hacer un relleno algo suelto para que la pasta tenga suficiente espacio y no se salga de la tripa. Se forman las salchichas individuales torciendo la tripa por tramos de 12 a 15am.

Horneado y ahumado

El secado se realiza a veces en una sala de oreo, antes de someterse a los hornos, en otros se realiza dentro de los hornos con aire caliente. El ahumado se realiza en hornos o cámaras de ahumado de distintos modelos o formas de ahumado.

Ahumado directo donde el humo se obtiene de quemas de aserrín o leña por debajo del producto. Este tiene la desventaja de que el humo y el calor no está distribuido uniformemente. Horno con movimiento de carros y con distribución de humo por medio de un sistema de ventilación y finalmente aquellos que tiene equipo automático para controlar todo el proceso térmico. (Secado, ahumado, cocción y enfriamiento).

El proceso de ahumado básicamente le desarrolla el color al embutido que se realiza después de la desnaturalización de la proteína. Los parámetros generales son: temperatura de ahumado entre 70 y 80 ºC dependiendo del grosor del embutido por tiempos entre 0.5 y 2 horas.

Cocción

Los embutidos escaldados se elaboran a partir de carne fresca y se someten a un proceso de cocción (escaldado) en agua caliente a 75-80ºC, por un tiempo que lo determina el grosor de los embutidos.

La cantidad de sal que se añade es de 2 a 3% y su calidad final depende mucho de las envolturas utilizadas, deben permitir los cambios de tamaño del embutido durante el rellenado, el escaldado, el ahumado y el enfriamiento.

Los principales embutidos escaldados que contempla el proyecto son: las salchichas, chorizos y la Mortadela

Enfriamiento

Después del tratamiento térmico, ahumado y/o cocción es necesario enfriar rápidamente para evitar el desarrollo de microorganismos y para evitar las mermas por evaporación de la superficie del producto. Es necesario enfriar rápidamente a temperatura ambiente, para luego pasar a las cámaras o a los locales de empaque.

Empaque Para Salchicha

Para la salchicha se empleará un embace denominado tripa artificial cuyos calibres (diámetro de la tripa) son muy diversos aunque el normal para este tipo es de 20 y 22 m. m, es necesario

utilizar este embace tanto por sus propiedades como para dar una mayor presentación al producto. Para la salchicha se empleará una segunda envoltura o empaque de polímero mixto

Almacenamiento y venta

Finalmente se acondiciona en una cámara de frío, detallando a qué temperatura, durante cuánto tiempo mínimo y máximo, qué control de humedad tendrá esa cámara y qué velocidad del aire (control de mermas).

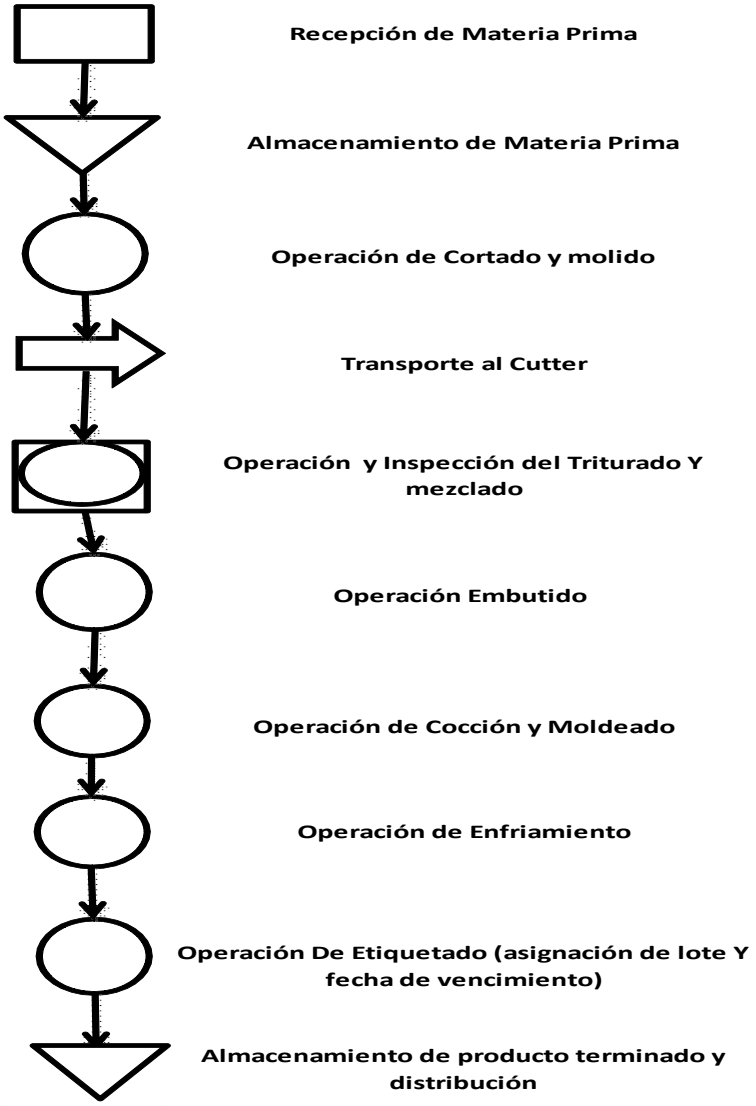


Figura 8: Diagrama de flujo de elaboración de mortadela de res

Almacenamiento de materia prima

Es un proceso en inicial en el cual se recepción la materia prima como ser: la carne de res el tocino en ambientes de refrigeración para que su conservación y así evitar una contaminación de microorganismos

Cortado y molido

Es un proceso previo de todo proceso de embutido, sobre todo cuando se aplica en la producción la carne congelada en bloque, que necesariamente deberá ser cortada en trozos por máquinas especiales llamadas guillotinas.

Por otro lado, cuando se preparan embutidos como la mortadela o jamonada, es necesario cortar la carne o la grasa (tocino) en cubos o trozos con determinadas dimensiones. En este caso se utilizan máquinas especiales de cortar.

Cuando es necesario moler la carne para elaborar productos, se utilizan molinos especiales que permiten tener diferentes grados de molido. En algunos casos la carne se muele primero mediante discos gruesos y después de salada, se muele mediante discos finos, o a veces se muelen una sola vez.

Cuando la carne es molida, se debe tener en cuenta que la temperatura del material molido no debe elevarse a más de 4 a 5 ºC de la temperatura inicial.

Emulsificación o trituración

En la mayoría de los embutidos se aplica la trituración de una parte de la masa cárnica o toda como por ejemplo chorizo, salame, etc; en otros se emulsifican una parte y los otros constituyentes (tocino, carne de cerdo, etc.) se pican o se muelen solo para garantizar una estructura específica.

Este proceso de emulsión es una destrucción mecánica de las fibras musculares y efectúa una liga o sea una emulsión entre la proteína muscular (miosina), la grasa y el agua.

Se debe controlar la cantidad de grasa en la emulsión, en relación con la fase proteína-agua. Y otro factor a controlar es la temperatura, por encima de 16ºC se desdobla o se rompe la emulsión.

La trituración y la emulsificación se realizan en máquinas especiales llamadas cutter; nombre que procede del inglés "tocut " es decir, cortar, que en realidad son máquinas de cortar y mezclar y cuyo principio de funcionamiento es: un plato o depósito que posee un movimiento rotativo, en el centro un vástago (eje) con un juego de cuchillas (de 2 a 12) en diferentes formas pero generalmente en forma de hoz, que giran a alta velocidad. El plato también se mueve a dos velocidades generalmente de 10 a 50 revoluciones por minuto. Las cuchillas giran a 4000 revoluciones por minuto. Algunas de estas máquinas pueden elaborar productos sin previo troceado o molido de la carne, y también poseen dispositivos automáticos suplementarios para carga y descarga mecánica y controles muy sofisticados.la masa, es recomendable que no suba de 10ºC. Las máquinas usadas son comúnmente llamadas mezcladoras, revolvedoras, amasadoras, etc.

Las mezcladoras en general constan de un depósito dentro de la cual giran en dirección contraria una de otras dos paletas montadas en ejes, con los cuales se puede cambiar la dirección de la rotación durante el trabajo. Poseen además un mecanismo de volteo del depósito.

Emulsificadores o molinos coloidales

Generalmente cuando se utilizan rellenos cárnicos como pellejos, bembos, tendones, etc., en productos como salchichas, patés, etc., en donde se necesita una buena trituración para lograr una emulsión estable se utilizan molinos coloidales, que permitan una finura que se puede variar.

Embutido y amarre

Independientemente de cómo se haya preparado la masa del producto ya sea en la cutter solamente o combinada en ésta y después en la mezcladora o simplemente en la mezcladora, la operación subsiguiente consiste en introducir o embutir esta masa cárnica en las tripas o moles correspondientes y realizar después el amarre final del producto

Para efectuar el proceso de embutido de la masa en tripas o moldes se utilizan máquinas especiales embutidoras, estas máquinas embuten la masa cárnica bajo presión tratando de mantener la calidad y la uniformidad de la distribución de los distintos componentes de la mezcla.

Existe una gran variedad de máquinas embutidoras, la embutidora clásica se compone de un cilindro dentro del cual se mueve un pistón se comprime la masa y la dirige hacia una salida donde se acopla una boquilla o embudo de medida y largo apropiados al grosor del producto.

Para el amarre de los productos se utilizan varios equipos que se acoplan a las máquinas embutidoras, uno de esos equipos son las clipsadoras que utilizan el alambre metálico para el amarre, otra forma son las máquinas torcedoras que generalmente el sistema está acoplado a la embutidora.

Por otro lado, existe una gran variedad de formas de amarrar los embutidos que se practica en cada país, cada una de ella en forma determinada a veces, con el propósito de distinguir las diferentes variedades de productos cárnicos.

Escaldado (cocción)

Los embutidos escaldados se elaboran a partir de carne fresca y se someten a un proceso de cocción (escaldado) en agua caliente a 75-80ºC, por un tiempo que lo determina el grosor de los embutidos.

La cantidad de sal que se añade es de 2 a 3% y su calidad final depende mucho de las envolturas utilizadas, deben permitir los cambios de tamaño del embutido durante el rellenado, el escaldado, el ahumado y el enfriamiento.

Los principales embutidos escaldados que contempla el proyecto son: El Hot dog, Jamón, Jamonada, y la Mortadela

Enfriamiento

Después del tratamiento térmico, ahumado y/o cocción es necesario enfriar rápidamente para evitar el desarrollo de microorganismos y para evitar las mermas por evaporación de la superficie del producto. Es necesario enfriar rápidamente a temperatura ambiente, para luego pasar a las cámaras o a los locales de empaque.

Almacenamiento y venta

Finalmente se acondiciona en una cámara de frío, detallando a qué temperatura, durante cuánto tiempo mínimo y máximo, qué control de humedad tendrá esa cámara y qué velocidad del aire (control de mermas).

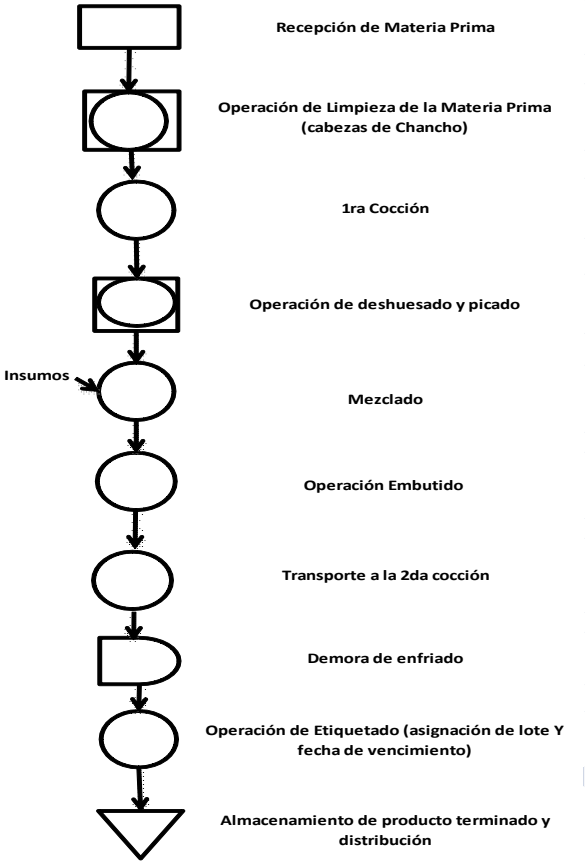


Figura 9: Diagrama de elaboración de queso de chancho

4.1.2.3 Descripción de la infraestructura e instalaciones de la unidad industrial

Infraestructura: La edificación está construida para el uso Familiar e industrial, la Superficie del lote es de 300 m^2. La empresa "EMBUTIDORA COPACABANA" se encuentra construido en una superficie de 142.50 m^2 conformado por las siguientes secciones:

SUPERFICIE $_{industria}$=142.50 (m2)

Planta baja: (Bloque de producción)

Este bloque está destinado para las siguientes actividades:

- Área de proceso
- Área de Cocción
- Almacén de materia prima
- Almacén de producto terminado
- Almacén de insumos

Planta Baja: (Ambientes administrativas)

Estos ambientes están destinados a las actividades administrativas.

Sala de espera

- Oficina
- Vestuarios

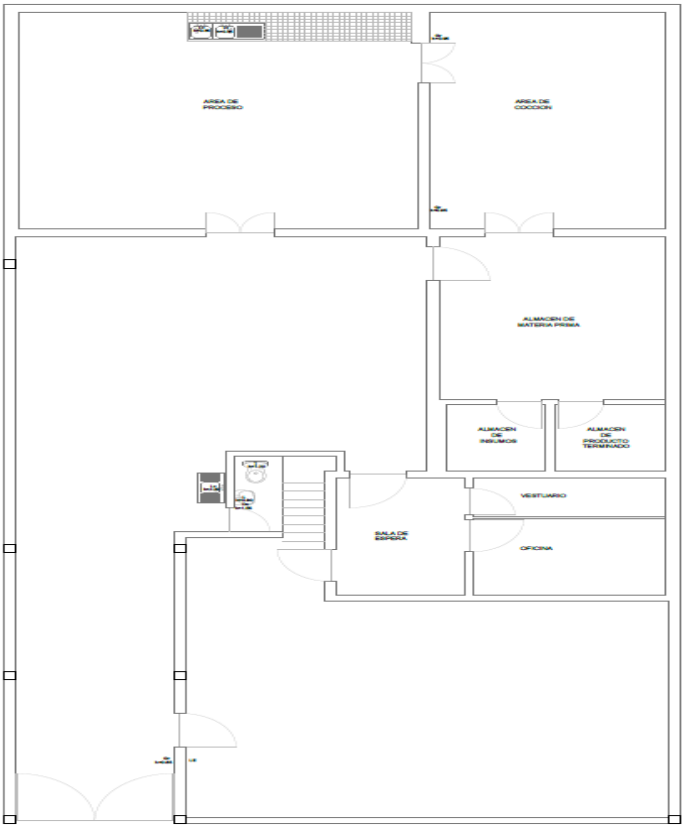


Figura 10: Plano de la empresa

4.1.2.4 Producción Industrial

La actividad productiva de la industria Embutidora “COPACABANA” es la elaboración de productos derivados de la carne de chancho

Tabla 5: Producción de derivados de chancho

PRODUCTO	UNIDAD	CANTIDAD
Queso de chancho	Kg	2400
Mortadela	Kg	200
Salchicha	Kg	100

Fuente: Elaboración Propia

Según datos proporcionados por la industria, las cantidades de fabricación de productos cárnicos, en los últimos tres meses se tiene un promedio de: Producción= 2700 (Kg/mes)

4.1.3 Criterios

El estudio del diseño de sistemas de seguridad electrónica basado en la norma ISO 31.000 para pequeñas empresas de alimentos de la ciudad de el alto" Caso: Embutidos Copacabana cuenta con las siguientes variables para el impactos y probabilidad obteniendo el nivel de riesgo en base a la entrevista y visita en las instalaciones de la empresa.

4.1.3.1 Probabilidad

En el siguiente cuadro se puede observar las variables de probabilidad y obtener el nivel de riesgo.

Tabla 6: Tabla de probabilidad

PROBABILIDAD		
Nivel	Variable	#
Improbable	Monetario	1
Posible	Monetario	2
Ocasional	Monetario	3
Probable	Monetario	4
Frecuente	Monetario	5

Fuente: Elaboración propia

4.1.3.2 Impacto

Tabla 7: Tabla de impacto

PROBABILIDAD		
Nivel	Variable	#
Insignificante	Tiempo	1
Menor	Tiempo	2
Moderado	Tiempo	3
Mayor	Tiempo	4
Catastrófico	Tiempo	5

Fuente: Elaboración propia

4.1.3.3 Matriz de Riesgo

Para el cálculo de niveles de riesgo a base de la fórmula de la estimación de riesgo aplicaremos la fórmula de la estimación de riesgo, en base a la probabilidad e impacto descritos en las anteriores tablas.

Tabla 8: Tabla de niveles de riesgo

NIVELES DE RIESGO	
PROBABILIDAD : IMPACTO	**NIVEL DE RIESGO**
1:1	Bajo
2:1	Bajo
3:1	Bajo
4:1	Bajo
1:2	Bajo
2:2	Bajo
1:3	Bajo
5:1	Medio
5:2	Medio
4:2	Medio
3:2	Medio
3:3	Medio
2:3	Medio
2:4	Medio
1:4	Medio
1:5	Medio
5:3	Alto
4:3	Alto
5:4	Alto
4:4	Alto
3:4	Alto
5:5	Alto
4:5	Alto
3:5	Alto
2:5	Alto

Fuente: Elaboración propia

Donde una vez realizado la estimación del riesgo podemos observar nuestro matriz de riesgo en base a los criterios definidos para la gestión de riesgo en los sistemas de seguridad electrónica

Figura 11: Criterio de Matriz de riesgos de Seguridad Electrónica

4.1.4 Evaluación del riesgo

4.1.4.1 Identificación de riesgos

En la primera etapa de identificación de riesgos se realizó la búsqueda de información donde se pudo evidenciar ciertos aspectos donde se tiene datos rescatados la falta de los sistemas de seguridad electrónica al mismo tiempo existe conocimientos de equipos y dispositivos de alarmas, sensores, sirenas, jaladores de emergencias, entro otros que permite la seguridad en las instalaciones en cualquier empresa.

De esta manera se puede evidenciar que la empresa dentro de sus instalaciones no contempla con varios equipos y sistemas que se necesita para el control y seguridad física de la empresa los cuales generan riesgos a la empresa los cuales ocasionará perdidas cuando los mismo se materialicen y los mismos de describen de acuerdo a las categorías de los sistemas de seguridad electrónica.

4.1.4.2 Sistema contra incendio

- Sistema contra incendio desactualizado
- Incendio en la empresa
- Lesiones a colaboradores de la empresa
- No alerta manual ante un accidente de incendio

- Falla en los dispositivos y equipos del sistema contra incendio
- Detección de falla en los dispositivos y equipos del sistema contra incendio
- Obsolescencia de equipos de sistemas contra incendios
- Desconocimiento ante una situación de incendios
- Sistema contra incendio aislada con sistemas de seguridad electrónica

4.1.4.3 Sistema de control de acceso

- Sistema de control de acceso desactualizado
- Acceso restringido a áreas de exclusión
- Ingreso de colaboradores en horarios fuera de oficina y/o feriado
- Falla en los dispositivos y equipos del sistema de control de accesos
- Obsolescencia de equipos de sistemas de control de accesos
- Detección de falla en los dispositivos y equipos del sistema de control de accesos
- Sistema de control de acceso aislada con sistemas de seguridad electrónica

4.1.4.4 Sistema de alarmas

- Sistema de control de alarmas desactualizado
- Intoxicación por gas
- Inundación interna
- Ingreso no autorizado a almacén y áreas de exclusión
- Daño de productos
- Falla en los dispositivos y equipos del sistema de alarmas
- Detección de falla en los dispositivos y equipos del sistema de alarmas
- Obsolescencia de equipos de sistemas de control de alarmas
- Sistema de alarmas aislada con sistemas de seguridad electrónica
- Activación de alarmas en horario fuera de trabajo

4.1.4.5 Circuitos Cerrado de Televisión CCTV

- Control de las instalaciones de la empresa de forma remota mediante cámaras
- Pruebas de incidentes
- Pruebas de robo
- Detección de falla en los dispositivos y equipos del sistema CCTV

- Falla en los dispositivos y equipos del sistema CCTV
- Verificación de obsolescencia de equipos de sistemas CCTV

4.1.5 Análisis del riesgo

Con la ayuda de revisión de estadística y entrevistas con la empresa de embutidos Copacabana se llegaron realizar las variables de Probabilidad e impacto para posteriormente poder obtener la valoración de los riesgos encontrados.

Tabla 9: Descripción de variable en probabilidad

PROBABILIDAD		
Nivel	Variable	#
Improbable	Sucede una vez en 1 años	1
Posible	Sucede una vez por semestre	2
Ocasional	Sucede una vez por trimestre	3
Probable	Sucede una vez por mes	4
Frecuente	Sucede varias veces en un mes	5

Fuente: Elaboración propia

Tabla 10: Descripción de variable de impacto

IMPACTO		
Nivel	Variable	#
Insignificante	Generaría pérdidas de 20 dólares o menos	1
Menor	Generaría pérdidas entre 21 y 100 dólares	2
Moderado	Generaría pérdidas entre 101 y 1.000 dólares	3
Mayor	Generaría pérdidas entre 1.001 y 5.000 dólares	4
Catastrófico	Generaría pérdidas de más de 50.000 dólares	5

Fuente: Elaboración propia

4.1.6 Valoración del riesgo

De acuerdo a los procesos descritos anteriormente se tiene el cuadro con la identificación de los riesgos encontrados de la siguiente manera, aplicando la fórmula de:

RIESGO = PROBABILIDAD X IMPACTO

Tabla 11: *Elaboración de valoración de riesgos encontrados*

N°	Identificación			Valoración					
	Causa	Riesgo	Categoría	¿Cada cuanto podría suceder?	¿Qué impacto podría causar?	Probabilidad	Impacto	Calificación de Riesgo	Nivel de Riesgo
1	Falta de actualización de sistema CCTV	Sistema contra incendio desactualizado	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto
2	Falta de sensores de humo	Incendio en la empresa	Sistema Contra Incendio	Sucede una vez por mes	Generaría pérdidas de más de 50.000 dólares	4	5	4:5	Alto
3	Falta de luz estroboscópicas para la salida de emergencias	Lesiones a colaboradores de la empresa	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo
4	Falta de jalador de emergencia ante incendios	No alerta manual ante un accidente de incendio	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas entre 1.001 y 5.000 dólares	1	4	1:4	Medio
5	No contar con mantenimientos programados a los equipos de sistema contra incendios	Falla en los dispositivos y equipos del sistema contra incendio	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
6	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema contra incendio	Detección de falla en los dispositivos y equipos del sistema contra incendio	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
7	No verificar el tiempo de vida util del dispositivo electrónico	Obsolescencia de equipos de sistemas contra incendios	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo
8	Falta de capacitación en el uso de los sistemas contra incendio a funcionarios	Desconocimiento ante una situación de incendios	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
9	Falta de Integración de sistema contra incendio con sistemas de seguridad electrónica	Sistema contra incendio aislada con sistemas de seguridad electrónica	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo
10	Falta de actualización de sistema de control de acceso	Sistema de control de acceso desactualizado	Sistema de Control de Acceso	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto
11	Falta de dispositivos de control de accesos como biométricos, lector de tarjetas o acceso por código de empleado	Acceso restringido a áreas de exclusión	Sistema de Control de Acceso	Sucede una vez por semestre	Generaría pérdidas entre 1.001 y 5.000 dólares	2	4	2:4	Medio
12	Falta de control de ingreso en horarios fuera de oficina y/ feriado	Ingreso de colaboradores en horarios fuera de oficina y/o feriado	Sistema de Control de Acceso	Sucede una vez por mes	Generaría pérdidas entre 101 y 1.000 dólares	4	3	4:3	Alto
13	No contar con mantenimientos programados a los equipos de control de accesos	Falla en los dispositivos y equipos del sistema de control de accesos	Sistema de Control de Acceso	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
14	No verificar el tiempo de vida útil del dispositivo electrónico de control de accesos	Obsolescencia de equipos de sistemas de control de accesos	Sistema de Control de Acceso	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
15	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema de control de accesos	Detección de falla en los dispositivos y equipos del sistema de control de accesos	Sistema de Control de Acceso	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo
16	Falta de Integración de sistema de control de acceso con sistemas de seguridad electrónica	Sistema de control de acceso aislada con	Sistema de Control	Sucede una vez en 1 años	Generaría pérdidas de 20	1	1	1:1	Bajo

		sistemas de seguridad electrónica	de Acceso		dólares o menos				
17	Falta de actualización de sistema de alarmas	Sistema de control de alarmas desactualizado	Sistema de Alarmas	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto
18	Falta de detectores de gases	Intoxicación por gas	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 1.001 y 5.000 dólares	5	4	5:4	Alto
19	Falta de detectores de aniego (agua)	Inundación interna	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas de 20 dólares o menos	5	1	5:1	Medio
20	Falta de detectores de movimiento	Ingreso no autorizado a almacén y áreas de exclusión	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas de 20 dólares o menos	5	1	5:1	Medio
21	Falta de sensores de temperatura	Daño de productos	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 101 y 1.000 dólares	5	3	5:3	Alto
22	No contar con mantenimientos programados a los equipos de sistemas de alarmas	Falla en los dispositivos y equipos del sistema de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
23	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema de alarmas	Detección de falla en los dispositivos y equipos del sistema de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
24	No verificar el tiempo de vida util del dispositivo electrónico de control de accesos	Obsolescencia de equipos de sistemas de control de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 101 y 1.000 dólares	2	3	2:3	Medio
25	Falta de Integración de sistema de alarmas con sistemas de seguridad electrónica	Sistema de alarmas aislada con sistemas de seguridad electrónica	Sistema de Alarmas	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo
26	Activación de sensores en horarios fuera de trabajo	Activación de alarmas en horario fuera de trabajo	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 21 y 100 dólares	5	2	5:2	Medio
27	No contar con sistema de circuito cerrado de televisión CCTV en las instalaciones	Control de las instalaciones de la empresa de forma remota mediante cámaras	Circuitos Cerrado de televisión	Sucede varias veces en un mes	Generaría pérdidas entre 101 y 1.000 dólares	5	3	5:3	Alto
28	No contar con cámaras que realicen grabaciones en lugares de camino de ronda y exclusión	Pruebas de incidentes	Circuitos Cerrado de televisión	Sucede una vez en 1 años	Generaría pérdidas entre 1.001 y 5.000 dólares	1	4	1:4	Medio
29	Con contar con grabaciones para evidencia	Pruebas de robo	Circuitos Cerrado de televisión	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	1:5	Medio
30	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema CCTV	Detección de falla en los dispositivos y equipos del sistema CCTV	Circuitos Cerrado de televisión	Sucede una vez por trimestre	Generaría pérdidas entre 101 y 1.000 dólares	3	3	3:3	Medio
31	No contar con mantenimientos programados a los equipos de sistemas CCTV	Falla en los dispositivos y equipos del sistema CCTV	Circuitos Cerrado de televisión	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo
32	No verificar el tiempo de vida util del dispositivo del sistema CCTV	Verificación de obsolescencia de equipos de sistemas CCTV	Circuitos Cerrado de televisión	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo

Fuente: Elaboración propia

En la siguiente figura que representa la matriz de riesgos se puede observar el cuadro resumen de los riesgos identificados en base la valoración para su tratamiento respectivo según a la criticidad.

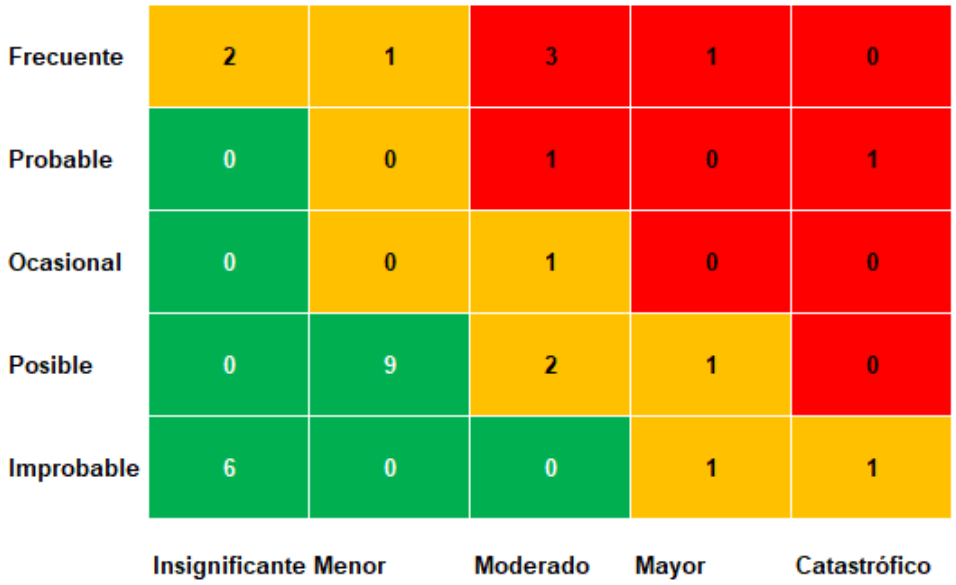


Figura 12: Matriz de riesgos obtenidos

4.1.7 Tratamiento del Riesgo

En base a las buenas prácticas de la norma ISO 31000, se realizó el tratamiento de los riesgos para su aceptación, eliminación, transferencia y mitigación como se muestra en la siguiente tabla.

Tabla 12: Tratamiento de los riesgos encontrados

No.	Identificación			Valoración						Tratamiento del Riesgo		
	Causa	Riesgo	Categoría	¿Cada cuanto podría suceder?	¿Qué impacto podría causar?	Probabilidad	Impacto	Calificación de Riesgo	Nivel de Riesgo	Tipo	Descripción Acción	Responsable
1	Falta de actualización de sistema CCTV	Sistema contra incendio desactualizado	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto	Mitigar	Compra de dispositivos de control electrónicos de sistema contra incendio	Gerente de la Empresa
2	Falta de sensores de humo	Incendio en la empresa	Sistema Contra Incendio	Sucede una vez por mes	Generaría pérdidas de más de 50.000 dólares	4	5	4:5	Alto	Mitigar	Instalación de dispositivos de sensores de humo en instalaciones de la empresa como almacenes, producción, ambientes de exclusión	Gerente de la Empresa
3	Falta de luz estroboscópicas para la salida de emergencias	Lesiones a colaboradores de la empresa	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo	Mitigar	Instalación de dispositivos de Luz Estroboscópicas a la salida de los ambientes de trabajo dentro la empresa para indicar la salida de las instalaciones en caso de una emergencia	Gerente de la Empresa
4	Falta de jalador de emergencia ante incendios	No alerta manual ante un	Sistema Contr	Sucede una vez	Generaría pérdidas	1	4	1:4	Medio	Mitig	Instalación de dispositivos de jaladores de emergencia asociados a las	Gerente de la

		accidente de incendio	a Incendio	en 1 años	entre 1.001 y 5.000 dólares					ar		Empresa
5	No contar con mantenimientos programados a los equipos de sistema contra incendios	Falla en los dispositivos y equipos del sistema contra incendio	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios de mantenimiento de sistemas de incendios	Gerente de la Empresa
6	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema contra incendio	Detección de falla en los dispositivos y equipos del sistema contra incendio	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios que realice pruebas a los dispositivos contra incendios	Supervisor de Producción
7	No verificar el tiempo de vida util del dispositivo electrónico	Obsolescencia de equipos de sistemas contra incendios	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo	Transferir	Tener registros de compra de los dispositivos de seguridad electronica de tal manera que cuanto pase la vida util activar una nueva compra por depreciación	Supervisor de Producción
8	Falta de capacitación en el uso de los sistemas contra incendio a funcionarios	Desconocimiento ante una situación de incendios	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Realización de capacitación de manejo de extintores y evacuaciones	Gerente de la Empresa
9	Falta de Integración de sistema contra incendio con sistemas de seguridad electrónica	Sistema contra incendio aislada con sistemas de seguridad electrónica	Sistema Contra Incendio	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo	Aceptar	Monitorear el sistema contra incendio independiente	Supervisor de Producción
10	Falta de actualización de sistema de control de acceso	Sistema de control de acceso desactualizado	Sistema de Control de Acceso	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto	Mitigar	Compra de dispositivos de control electrónicos de control de accesos	Gerente de la Empresa
11	Falta de dispositivos de control de accesos como biométricos, lector de tarjetas o acceso por código de empleado	Acceso restringido a áreas de exclusión	Sistema de Control de Acceso	Sucede una vez por semestre	Generaría pérdidas entre 1.001 y 5.000 dólares	2	4	2:4	Medio	Mitigar	Instalación de dispositivos de control de acceso en ambientes de restricción	Gerente de la Empresa
12	Falta de control de ingreso en horarios fuera de oficina y/ feriado	Ingreso de colaboradores en horarios fuera de oficina y/o feriado	Sistema de Control de Acceso	Sucede una vez por mes	Generaría pérdidas entre 101 y 1.000 dólares	4	3	4:3	Alto	Mitigar	Instalación de contactos magnéticos programados con alertas de ingreso fuera de hora	Gerente de la Empresa
13	No contar con mantenimientos programados a los equipos de control de accesos	Falla en los dispositivos y equipos del sistema de control de accesos	Sistema de Control de Acceso	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios de mantenimiento de sistemas de control de acceso	Supervisor de Producción
14	No verificar el tiempo de vida útil del dispositivo electrónico de control de accesos	Obsolescencia de equipos de sistemas de control de accesos	Sistema de Control de Acceso	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Tener registros de compra de los dispositivos de control de acceso de tal manera que cuanto pase la vida util activar una nueva compra por depreciación	Supervisor de Producción

15	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema de control de accesos	Detección de falla en los dispositivos y equipos del sistema de control de accesos	Sistema de Control de Acceso	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo	Transferir	Contratar un proveedor de servicios que realice pruebas a los dispositivos de control de acceso	Supervisor de Producción
16	Falta de Integración de sistema de control de acceso con sistemas de seguridad electrónica	Sistema de control de acceso aislada con sistemas de seguridad electrónica	Sistema de Control de Acceso	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo	Aceptar	Monitorear el sistema de control de acceso	Supervisor de Producción
17	Falta de actualización de sistema de alarmas	Sistema de control de alarmas desactualizado	Sistema de Alarmas	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto	Mitigar	Compra de dispositivos de control electrónicos de sistemas de alarmas	Gerente de la Empresa
18	Falta de detectores de gases	Intoxicación por gas	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 1.001 y 5.000 dólares	5	4	5:4	Alto	Mitigar	Instalación de sensor de gas "GLP"	Gerente de la Empresa
19	Falta de detectores de aniego (agua)	Inundación interna	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas de 20 dólares o menos	5	1	5:1	Medio	Mitigar	Instalación de sensor de aniego para detección de agua	Gerente de la Empresa
20	Falta de detectores de movimiento	Ingreso no autorizado a almacén y áreas de exclusión	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas de 20 dólares o menos	5	1	5:1	Medio	Mitigar	Instalación de detectores de movimiento en lugares restringidos de la empresa para la verificación de intrusos	Gerente de la Empresa
21	Falta de sensores de temperatura	Daño de productos	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 101 y 1.000 dólares	5	3	5:3	Alto	Mitigar	Instalación de sensores de temperatura en los almacenes de productos y materia prima para no tener daños	Gerente de la Empresa
22	No contar con mantenimientos programados a los equipos de sistemas de alarmas	Falla en los dispositivos y equipos del sistema de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios de mantenimiento de sistemas de alarmas	Supervisor de Producción
23	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema de alarmas	Detección de falla en los dispositivos y equipos del sistema de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios que realice pruebas a los dispositivos de alarmas	Supervisor de Producción
24	No verificar el tiempo de vida util del dispositivo electrónico de control de accesos	Obsolescencia de equipos de sistemas de control de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 101 y 1.000 dólares	2	3	2:3	Medio	Transferir	Tener registros de compra de los dispositivos de alarmas de tal manera que cuanto pase la vida útil activar una nueva compra por depreciación	Supervisor de Producción
25	Falta de Integración de sistema de alarmas con sistemas de seguridad electrónica	Sistema de alarmas aislada con sistemas de seguridad electrónica	Sistema de Alarmas	Sucede una vez en 1 años	Generaría pérdidas de 20 dólares o menos	1	1	1:1	Bajo	Aceptar	Monitorear el sistema de alarmas	Supervisor de Producción

26	Activación de sensores en horarios fuera de trabajo	Activación de alarmas en horario fuera de trabajo	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 21 y 100 dólares	5	2	5:2	Medio	Mitigar	Monitoreo constante de todas las alarmas de manera diaria para ver los eventos en la empresa de acuerdo al tipo de alarma activada	Supervisor de Producción
27	No contar con sistema de circuito cerrado de televisión CCTV en las instalaciones	Control de las instalaciones de la empresa de forma remota mediante cámaras	Circuitos Cerrado de televisión	Sucede varias veces en un mes	Generaría pérdidas entre 101 y 1.000 dólares	5	3	5:3	Alto	Mitigar	Compra de licencia para visualización remota desde dispositivos móviles, con dispositivos de vigilancia cámaras y dvr	Gerente de la Empresa
28	No contar con cámaras que realicen grabaciones en lugares de camino de ronda y exclusión	Pruebas de incidentes	Circuitos Cerrado de televisión	Sucede una vez en 1 años	Generaría pérdidas entre 1.001 y 5.000 dólares	1	4	1:4	Medio	Mitigar	Instalación de cámaras de seguridad en el ambiente de producción de la empresa	Gerente de la Empresa
29	Con contar con grabaciones para evidencia	Pruebas de robo	Circuitos Cerrado de televisión	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	1:5	Medio	Mitigar	Instalación de cámaras de seguridad en los almacenes y equipos de la empresa	Gerente de la Empresa
30	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema CCTV	Detección de falla en los dispositivos y equipos del sistema CCTV	Circuitos Cerrado de televisión	Sucede una vez por trimestre	Generaría pérdidas entre 101 y 1.000 dólares	3	3	3:3	Medio	Transferir	Contratar un proveedor de servicios que realice pruebas a los dispositivos de CCTV	Supervisor de Producción
31	No contar con mantenimientos programados a los equipos de sistemas CCTV	Falla en los dispositivos y equipos del sistema CCTV	Circuitos Cerrado de televisión	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios de mantenimiento de sistemas CCTV	Supervisor de Producción
32	No verificar el tiempo de vida util del dispositivo del sistema CCTV	Verificación de obsolescencia de equipos de sistemas CCTV	Circuitos Cerrado de televisión	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Tener registros de compra de los dispositivos de CCTV de acceso de tal manera que cuanto pase la vida útil activar una nueva compra por depreciación	Supervisor de Producción

Fuente. Elaboración propia

4.1.8 Registro e Informe

Para la realización del informe se utilizó el cuadro de tratamiento de riesgo elaborado en el anterior punto donde se detalla los registros de las causas, los riesgos, su clasificación, variables de probabilidad e impacto, nivel de riesgo, tipo de tratamiento, acciones a realizar y como ultimo los responsables de realizar dichas acciones, el informe y registro se puede observar en el informe emitido a la empresa de alimentación de Embutidos Copacabana quienes pueden realizan los gastos de implementación para la mitigación de los riesgos encontrados. Ver (Anexo 5).

4.2 Diseño de Sistemas de Seguridad Electrónica para Pequeñas Empresas de Alimentos de la ciudad de El Alto

En base a la recolección de información recolectada y con el caso de estudio de la empresa de alimentos embutidos Copacabana.

Se realizo el siguiente diseño de los sistemas de seguridad electrónica en base a la norma ISO 31000.

La pequeña empresa de alimentos, debe constituir un sistema para la Gestión de Seguridad Electrónica en base a la norma ISO 31.000, que permita identificar, monitorear, controlar y mitigar en forma preventiva o correctiva, impidiendo y/o neutralizando los riesgos a incidentes de seguridad física y sus consecuencias.

La pequeña empresa debe realizar un análisis de riesgos de seguridad electrónica, con base en el cual se determine el nivel de riesgo ante incidentes de seguridad al que se encuentra expuesto. Este análisis de riesgos en seguridad electrónica debe ser efectuado al menos una vez al año para reducir el nivel de riesgo.

Las pequeñas empresas deben contener al menos deben contemplar en los sistemas de seguridad electrónica de gama media los siguientes dispositivos.

Las pequeñas empresas de alimentos deben contemplar al menos algunos dispositivos primordiales en cada uno de los sistemas de seguridad para su funcionamiento:

Sistema de Contra Incendios

La empresa debe contar con un sistema contra incendio manual y automatizada a través de una central debidamente instalada que permita realizar la supervisión de todos los dispositivos programados, interconectado a una central de monitoreo de alarma y habilitados para detectar incidentes de incendio en áreas de producción, almacenes y áreas de exclusión que hubieran sido identificadas como resguardo de mayor importancia, los dispositivos mínimos son:

- Jaladores de emergencia
- Detectores de humo

- Sirenas con luces estroboscópicas
- Extintores
- Señaléticas de aviso de seguridad
- Central de alarmas

Estos dispositivos deben ser colocados de acuerdo a la infraestructura donde los colaboradores de cada empresa tengan acceso visible y uso de estos elementos.

Sistema de Control de Acceso

La empresa debe contar con un sistema control de acceso manual y/o automatizada a través de una central debidamente instalada que permita realizar la supervisión de todos los dispositivos conectados, para detectar ingresos a las áreas de la empresa como producción, almacenes y áreas de exclusión que hubieran sido identificadas como resguardo de mayor importancia, los dispositivos mínimos son:

- Chapa magnética
- Lector de entrada como:
  - Biométrico
  - Lector de tarjetas de aproximación
  - Código de teclado
  - NFC
  - Facial

Estos dispositivos deben ser colocados de acuerdo a la infraestructura donde los colaboradores de cada empresa tengan acceso a las áreas de exclusión de la empresa.

Sistema de alarma

La empresa debe contar con un sistema de alarma debidamente instalado que permita realizar la supervisión de todos los dispositivos programados, interconectado a una central de monitoreo de alarma y habilitados para detectar incidentes de seguridad física en áreas de producción, almacenes y áreas de exclusión que hubieran sido identificadas como resguardo de mayor importancia, los dispositivos mínimos son:

- Sensores de movimiento

- Detectores de humedad
- Detectores de temperatura
- Detectores de agua
- Detectores de gases
- Sensores de golpe
- Contactos magnéticos
- Sirenas
- Central de alarmas

Estos dispositivos deben ser colocados de acuerdo a la infraestructura de cada empresa debido que la seguridad es a ajustable a los ambientes y tiene que ser diseñado a medida de la empresa.

Sistema de Circuito Cerrado de Televisión CCTV

La empresa debe contar con un sistema de circuito cerrado de televisión CCTV control automatizado a través de una central debidamente instalada que permita realizar la supervisión a todas las cámaras instaladas en la empresa los dispositivos mínimos son:

- Cámaras
- Grabadora de videos
- Sistema de administración de cámaras

Estos dispositivos deben ser colocados de acuerdo a la infraestructura donde los colaboradores de cada empresa en lugares de camino de ronda y seguridad de las instalaciones y no así para el hostigamiento, acoso y control de los trabajadores de la empresa.

De acuerdo lo descrito se tiene el siguiente diseño para las empresas de seguridad electrónica en la siguiente imagen.

Figura 13: Diseño de sistema de seguridad electrónica para pequeña empresa de alimentos

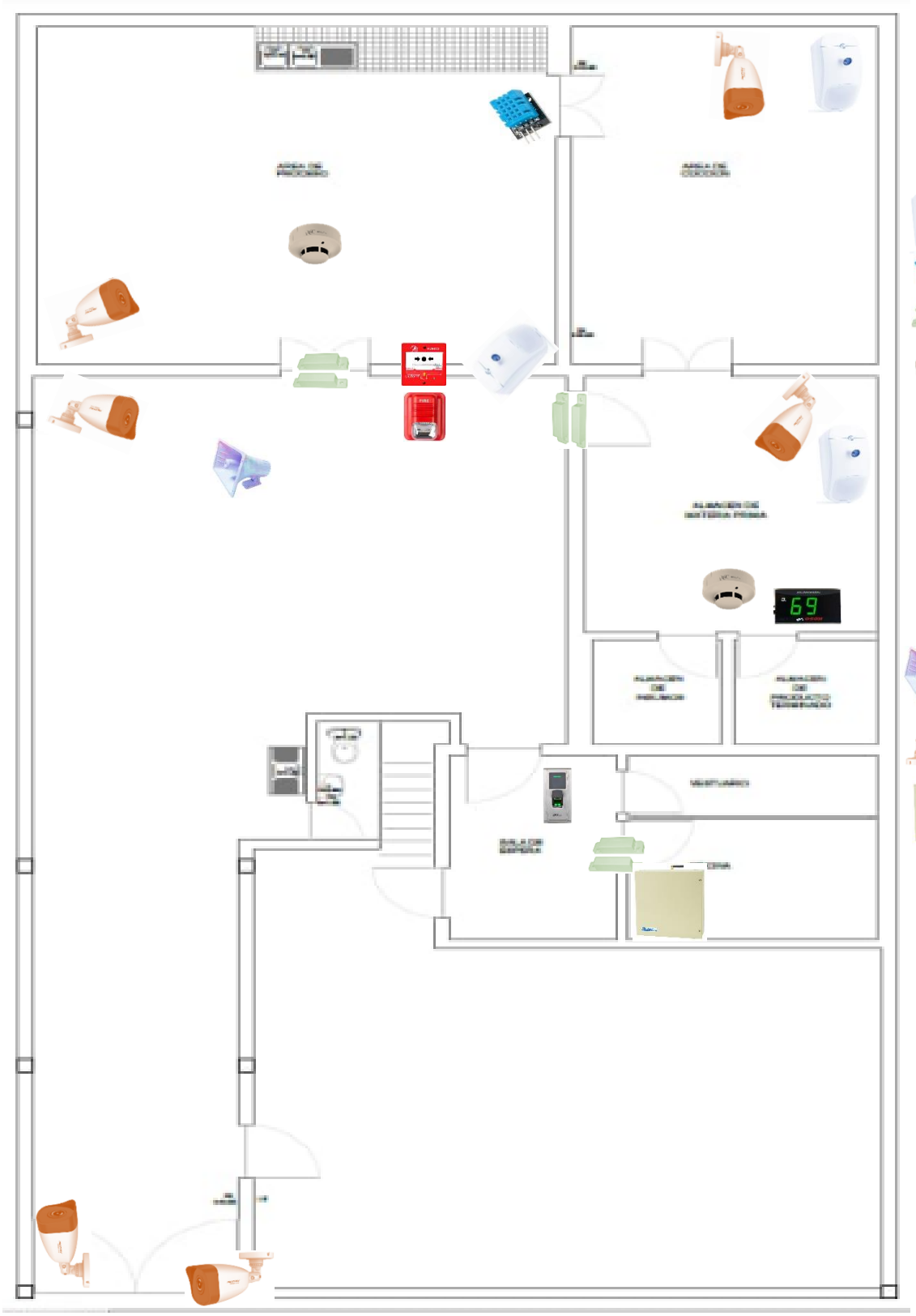


Figura 14: Diseño de instalación de dispositivos de seguridad en pequeñas empresas de alimentos

4.3 Resultados de la aplicación del diseño del sistema de seguridad electrónica

Una vez presentado el registro e informe correspondiente la empresa de Embutidos Copacabana en la necesidad de asegurar los ambientes físicos e infraestructura, decidido tratar algunos riesgos en relación a los sistemas de seguridad electrónica.

El total de los riesgos encontrados en la empresa fueron de 32 la empresa según los criterios y criticidad de tratamiento fueron aplicados 6 como se muestra en la siguiente tabla, reduciendo en un total de 19% los riesgos en la empresa.

Tabla 13: Lista de riesgos tratados

N°	Identificación			Valoración						Tratamiento del Riesgo			
	Causa	Riesgo	Categoría	¿Cada cuanto podría suceder?	¿Qué impacto podría causar?	Probabilidad	Impacto	Calificación de Riesgo	Nivel de Riesgo	Tipo	Descripción Acción	Responsable	% DE EJECUCIÓN
8	Falta de capacitación en el uso de los sistemas contra incendio a funcionarios	Desconocimiento ante una situación de incendios	Sistema Contra Incendio	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Realización de capacitación de manejo de extintores y evacuaciones	Gerente de la Empresa	100 %
17	Falta de actualización de sistema de alarmas	Sistema de control de alarmas desactualizado	Sistema de Alarmas	Sucede una vez en 1 años	Generaría pérdidas de más de 50.000 dólares	1	5	0.1	Alto	Mitigar	Compra de dispositivos de control electrónicos de sistemas de alarmas	Gerente de la Empresa	100 %
20	Falta de detectores de movimiento	Ingreso no autorizado a almacén y áreas de exclusión	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas de 20 dólares o menos	5	1	5:1	Medio	Mitigar	Instalación de detectores de movimiento en lugares restringidos de la empresa para la verificación de intrusos	Gerente de la Empresa	100 %
22	No contar con mantenimientos programados a los equipos de sistemas de alarmas	Falla en los dispositivos y equipos del sistema de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios de mantenimiento de sistemas de alarmas	Supervisor de Producción	100 %
23	No realizar pruebas de funcionamiento de equipos, dispositivos del sistema de alarmas	Detección de falla en los dispositivos y equipos del sistema de alarmas	Sistema de Alarmas	Sucede una vez por semestre	Generaría pérdidas entre 21 y 100 dólares	2	2	2:2	Bajo	Transferir	Contratar un proveedor de servicios que realice pruebas a los dispositivos de alarmas	Supervisor de Producción	100 %
26	Activación de sensores en horarios fuera de trabajo	Activación de alarmas en horario fuera de trabajo	Sistema de Alarmas	Sucede varias veces en un mes	Generaría pérdidas entre 21 y 100 dólares	5	2	5:2	Medio	Mitigar	Monitoreo constante de todas las alarmas de manera diaria para ver los eventos en la empresa de acuerdo al tipo de alarma activada	Supervisor de Producción	100 %

Fuente: Elaboración propia

La en el tratamiento de los riesgos se realizó la instalación de dispositivos y sistema de seguridad electrónica con el software **ELDES Security App** que es monitoreado a través de una cuenta de administración de alarmas de manera remota haciendo que el responsable este monitoreando las alarmas que vayan reportando.

Figura 15: Software de control de sistemas de alarmas

Figura 16: Dispositivos instalados del sistema de alarmas

CAPITULO V: CONCLUSIONES

Considerando las pequeñas empresas de alimentos en la ciudad de en la Ciudad de El Alto, gracias al apoyo de la empresa de Embutidos Copacabana en la cual el presente proyecto de investigación de “DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO” se tiene las siguientes conclusiones.

- Las pequeñas empresas de alimentos no cuentan con una metodología que permia Identificar los riesgos en los sistemas de seguridad electrónica en pequeñas empresas de alimentos.

  Con el diseño de elaborado en base a la norma ISO 31.000:2018 se logró identificar los riesgos de seguridad electrónica para su tratamiento a medida de la empresa pueda entrar con la implementación de los controles adecuados según las recomendaciones.
- En base de la elaboración de identificación de los riesgos identificados en primera instancia se realizó el análisis y valoración los riesgos identificados para su tratamiento de acuerdo a las recomendaciones del informe realizado.

  Este tratamiento y su implementación dependerá en medida de las posibilidades de la empresa, no dejando en cuenta que al mismo tiempo se puede tener algunos controles para no dejar de lado los riesgos identificados para su constante supervisión.
- En base a la información de los dispositivos que componen los sistemas de seguridad electrónica y la norma ISO 31.000 se elaboró un diseño sistemas de seguridad electrónica para pequeñas empresas de alimentos de la ciudad de el alto.
- En la construcción del diseño de Sistemas De Seguridad Electrónica Basado en la Norma ISO 31.000 para pequeñas Empresas de Alimentos de la ciudad de El Alto se trabajó con la empresa de Embutidos Copacabana el cual permitió en base el contexto de la ciudad de El Alto y la empresa definir criterios, alcances que lograron la identificación de riesgos, su análisis, valoración y tratamiento de los mismos respaldado en un informe el cual con la empresa está realizando las gestiones para minimizar los riesgos más elevados encontrando en tal sentido el diseño elaborado aplicado en esta empresa servirá como apoyo en empresas del mismo rubro.
- Una vez presentado el informe a la empresa la misma decidió realizar el tratamiento de algunos riesgos que minimicen el porcentaje global encontrado, de esa manera se aplicó la solución de diseño de seguridad electrónica planteado reduciendo un total de

19% de los riesgos encontrados con la instalación de dispositivos de seguridad electrónica como se ve en tabla N° 13 en el capítulo IV Resultados.

- En relación al análisis de la hipótesis “El diseño propuesto para los sistemas de seguridad electrónica basado en la norma ISO 31000 reduce los riegos de seguridad en pequeñas empresas de alimentos la ciudad de El Alto”, con el diseño planteado en la investigación y con la aplicación del diseño de sistemas de seguridad electrónica basado en la norma ISO 31.000 para pequeñas empresas de alimentos reduciendo un 19% en los riesgos encontrados se acepta la hipótesis planteada.

CAPITULO VI: RECOMENDACIONES

Efectuada el estudio de investigación, consideramos pertinente plantear las siguientes recomendaciones y sugerencias.

- Para la implementación de los sistemas de seguridad electrónica es importante que la empresa conozca el valor de sus activos que tiene en su infraestructura como maquinaria, áreas de exclusión, área de producción y almacén de sus artículos y de esa manera asegurar los mismos con sistemas y mecanismos que se tiene en la actualidad.

- Para involucrar aún más a la empresa se tiene que realizar capacitaciones en relación a los sistemas de seguridad electrónica y los dispositivos que estos tienen y en qué sentido puede ayudar a fortalecer el aseguramiento de los activos de la empresa.

- Para la implementación del diseño de Sistemas de Seguridad Electrónica basado en la norma ISO 31.000, las pequeñas empresas de alimentos de la ciudad de El Alto, tiene que tener en cuenta que estos sistemas se pueden implementar de manera incremental dependiendo a los riesgos más críticos que se pueda identificar.

- A la empresa de embutidos Copacabana seguir con el tratamiento de los riesgos encontrados bajo el diseño de seguridad electrónica realizado en la investigación de tal manera mejore su aseguramiento de las instalaciones e infraestructura de la empresa.

BIBLIOGRAFIA

Capistrano, J. B. (2019). Desarrollo de un Sistema de Seguridad. Lima, Peru.

LUCERO GÓMEZ, A. J., & VALVERDE PADILLA, J. O. (2012). ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGIA MAGERIT. *ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGIA MAGERIT*. Cuenca, Ecuador.

Mora, L. (2016). Conferencia anual latinoamericana sobre delitos financieros de la ACFCS. *Guia practica - Armado de una precisa matriz de riesgos*, (pág. 29). Panamá.

Online Browsing Platform (OBP). (16 de noviembre de noviembre de 2022). Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Paillacho Arias, S. M. (Marzo de 2015). Modelo de un proceso de la gestión del riesgo de la seguridad de la información en entidades gubernamentales. Quito, Ecuador: Escuela Politécnica Nacional.

RIVAS CRUZ, J. A., & VELAZQUEZ VILLA, C. A. (noviembre de 2011). IMPLEMENTACIÓN DE SISTEMA DE SEGURIDAD CON VIDEO-VIGILANCIA Y SOFTWARE LIBRE. D.F., Mexico.

Roca Chillida, J. M. (2018). *http://www.informeticplus.com/*. Obtenido de http://www.informeticplus.com/que-es-la-seguridad-electronica

Rosero Gómez, Á. R. (2108). Inclusión de la Gestión del Riesgo de Desastres en los diferentes niveles de GAD del Ecuador considerando la relación entre el marco legal existente y prácticas populares tradicionales. Ecuaador.

RUDAS TAYO, L. P. (31 de julio de 2017). MODELO DE GESTION DE RIESGOS PARA PROYECTOS DE DESARROLLO TECNOLOGICO. SANTIAGO DE QUERETARO, MEXICO.

ANEXOS

Anexo 1.- Registro Senapi: Resolución Administrativa NRO. 1-2958/2022

senapi
SERVICIO NACIONAL DE PROPIEDAD INTELECTUAL

ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE DESARROLLO PRODUCTIVO Y ECONOMÍA PLURAL

SERVICIO NACIONAL DE PROPIEDAD INTELECTUAL
DERECHO DE AUTOR Y DERECHOS CONEXOS
senapi

2022-TLIT-1134-0-1

DIRECCIÓN DE DERECHO DE AUTOR
Y DERECHOS CONEXOS
RESOLUCIÓN ADMINISTRATIVA NRO. 1-2958/2022
La Paz, 13 de Diciembre del 2022

VISTOS:

La solicitud de Inscripción de Derecho de Autor presentada en fecha **7 de Diciembre del 2022**, por **RONALDO RENE NINA TINTA** con **C.I. Nº 6045127 LP**, con número de trámite **DA 1379/2022**, señala la pretensión de inscripción de la Compilación de Obras Escritas titulada: **"PROYECTOS DE INVESTIGACIÓN UPEA GESTIÓN 2022 - INSTITUTO DE INVESTIGACIÓN Y POSGRADO INGENIERÍA EN PRODUCCIÓN EMPRESARIAL"**, conformada por las Obras Escritas: **"DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA"**, **"METODOLOGÍA MODERNA DE OPTIMIZACIÓN EN UN SISTEMA DE PRODUCCIÓN BASADA EN EL SOFTWARE DE SIMULACIÓN FLEXSIM". CASO: FRANSPORT PYME TEXTÍL CONFECCIÓN DE LA CIUDAD DE EL ALTO"** y **"DISTRIBUCIÓN GEOGRÁFICA, POTENCIAL PRODUCTIVO Y ALTERNATIVAS DE COMERCIALIZACIÓN DEL NOPAL (Opuntia ficus indica) EN DOS COMUNIDADES DEL CANTON SAPAHAQUI DEL DEPARTAMENTO DE LA PAZ"**, cuyos datos y antecedentes se encuentran adjuntos y expresados en los Formularios de Solicitud, documentación que tiene la calidad de Declaración Jurada.

CONSIDERANDO

Que, en observación al Artículo 4º del Decreto Supremo Nº 27938 modificado parcialmente por el Decreto Supremo Nº 28152 el *"Servicio Nacional de Propiedad Intelectual SENAPI, administra en forma desconcentrada e integral el régimen de la Propiedad Intelectual en todos sus componentes, mediante una estricta observancia de los regímenes legales de la Propiedad Intelectual, de la vigilancia de su cumplimiento y de una efectiva protección de los derechos de exclusiva referidos a la propiedad industrial, al derecho de autor y derechos conexos; constituyéndose en la oficina nacional competente respecto de los tratados internacionales y acuerdos regionales suscritos y adheridos por el país, así como de las normas y regímenes comunes que en materia de Propiedad Intelectual se han adoptado en el marco del proceso andino de integración"*.

Que, el Artículo 16º del Decreto Supremo Nº 27938 establece *"Como núcleo técnico y operativo del SENAPI funcionan las Direcciones Técnicas que son las encargadas de la evaluación y procesamiento de las solicitudes de derechos de propiedad intelectual, de conformidad a los distintos regímenes legales aplicables a cada área de gestión"*. En ese marco, la Dirección de Derecho de Autor y Derechos Conexos otorga registros con carácter declarativo sobre las obras del ingenio cualquiera que sea el género o forma de expresión, sin importar el mérito literario o artístico a través de la inscripción y la difusión, en cumplimiento a la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina, Ley de Derecho de Autor Nº 1322, Decreto Reglamentario Nº 23907 y demás normativa vigente sobre la materia.

Que, la solicitud presentada cumple con: el Artículo 6º de la Ley Nº 1322 de Derecho de Autor, el Artículo 26º inciso a) del Decreto Supremo Nº 23907 Reglamento de la Ley de Derecho de Autor, y con el Artículo 4º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina.

Que, de conformidad al Artículo 18º de la Ley Nº 1322 de Derecho de Autor en concordancia con el Artículo 18º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina, referentes a la duración de los Derechos Patrimoniales, los mismos establecen que: *"la duración de la protección concedida por la presente ley será para toda la vida del autor y por 50 años después de su muerte, a favor de sus herederos, legatarios y cesionarios"*.

V°B° Ing. Carlos Alberto Cahuaya Arroyo SENAPI

V°B° Henry Cahuaya Quino SENAPI

NB/ISO 9001 IBNORCA Signos Distintivos

"2022 AÑO DE LA REVOLUCIÓN CULTURAL PARA LA DESPATRIARCALIZACIÓN:
POR UNA VIDA LIBRE DE VIOLENCIA CONTRA LAS MUJERES"

HECHO EN BOLIVIA

Oficina Central - La Paz
Av. Montes, No 515, entre Esq. Uruguay y C. Batallón Illimani, Telfs.: 2115700 - 2119276 2119251 Fax: 2115700

Oficina - Santa Cruz
Av. Uruguay, Calle prolongación Quijarro, Nº 29, Edif. Bicentenario. Telfs.: 3121752 - 72042936

Oficina - Cochabamba
Calle Chuquisaca, Nº 649, Piso 2, entre Antezana y Lanza zona Central - Noreste. Telfs.: 4141403 - 72042957

Oficina - El Alto
Av. Juan Pablo II, Nº 2560 Edif. Multicentro El Ceibo Ltda. Piso 2, Of. 5B, zona 16 de Julio. Telfs.: 2141001 - 72043029

Oficina - Chuquisaca
Calle Kilómetro 7, Nº 366 casi esq. Urriolagoitia, zona Parque Bolivar. Telf.: 72005873

Oficina - Tarija
Calle Ingavi, Nº 385 entre Santa Cruz y Méndez, zona La Pampa. Telf.: 72015286

Oficina - Oruro
Calle 6 de Octubre, Nº 5837, entre Ayacucho y Junín, Galería Central, Of. 14 (Ex Banco Fie). Telf.: 67201288

Oficina - Potosí
Av. Villazón entre calles Wenceslao Alba y San Alberto, Edif. AM. Salinas Nº 242, Primer Piso, Of. 17.

www.senapi.gob.bo

senapi
SERVICIO NACIONAL DE PROPIEDAD INTELECTUAL

ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE DESARROLLO PRODUCTIVO Y ECONOMÍA PLURAL

Que, se deja establecido en conformidad al Artículo 4º de la Ley Nº 1322 de Derecho de Autor, y Artículo 7º de la Decisión 351 Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comunidad Andina que: *"...No son objeto de protección las ideas contenidas en las obras literarias, artísticas, o el contenido ideológico o técnico de las obras científicas ni su aprovechamiento industrial o comercial".*

Que, el artículo 4, inciso e) de la ley 2341 de Procedimiento Administrativo, instituye que: *"... en la relación de los particulares con la Administración Pública, se presume el principio de buena fe. La confianza, la cooperación y la lealtad en la actuación de los servidores públicos y de los ciudadanos ..."*, por lo que se presume la buena fe de los administrados respecto a las solicitudes de registro y la declaración jurada respecto a la originalidad de la obra.

POR TANTO

El Director de Derecho de Autor y Derechos Conexos.sin ingresar en mayores consideraciones de orden legal, en ejercicio de las atribuciones conferidas

RESUELVE:

INSCRIBIR en el Registro de Obras Escritas de la Dirección de Derecho de Autor y Derechos Conexos, la Compilación de Obras Escritas titulada: **"PROYECTOS DE INVESTIGACIÓN UPEA GESTIÓN 2022 - INSTITUTO DE INVESTIGACIÓN Y POSGRADO INGENIERÍA EN PRODUCCIÓN EMPRESARIAL"**, conformada por las Obras Escritas:

- **"DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA"**, a favor de los autores: **POLY LAZARO ISAAC SALAZAR LARICO** con **C.I. Nº 6818266 LP, JESUS CRISTIAN CALLE AVIRCATA** con **C.I. Nº 10076395 LP** y **ESTEFANI ESCURRA CABRERA** con **C.I. Nº 12731719 LP** y como titular derivado: **INSTITUTO DE INVESTIGACIONES INGENIERÍA EN PRODUCCIÓN EMPRESARIAL, UNIVERSIDAD PÚBLICA DE EL ALTO - UPEA** con **NIT Nº 122025022,** representado legalmente por **CARLOS CONDORI TITIRICO.**
- **"METODOLOGÍA MODERNA DE OPTIMIZACIÓN EN UN SISTEMA DE PRODUCCIÓN BASADA EN EL SOFTWARE DE SIMULACIÓN FLEXSIM". CASO: FRANSPORT PYME TEXTÍL CONFECCIÓN DE LA CIUDAD DE EL ALTO"** a favor de los autores: **WALTER JACINTO YUCRA** con **C.I. Nº 4823214 LP, BRAYAN MAMANI CRUZ** con **C.I. Nº 8382730 LP** y **JUAN JAVIER CERDANO LLUTA** con **C.I. Nº 9258539 LP** y como titular derivado: **INSTITUTO DE INVESTIGACIONES INGENIERÍA EN PRODUCCIÓN EMPRESARIAL, UNIVERSIDAD PÚBLICA DE EL ALTO - UPEA** con **NIT Nº 122025022** representado legalmente por **CARLOS CONDORI TITIRICO.**
- **"DISTRIBUCIÓN GEOGRÁFICA, POTENCIAL PRODUCTIVO Y ALTERNATIVAS DE COMERCIALIZACIÓN DEL NOPAL (Opuntia ficus indica) EN DOS COMUNIDADES DEL CANTON SAPAHAQUI DEL DEPARTAMENTO DE LA PAZ"** a favor de los autores: **MILTON VICTOR PINTO PORCEL** con **C.I. Nº 3458576 LP, JORGE LUIS VILLA CRUZ** con **C.I. Nº 12991738 LP** y **MARCO ANTONIO MAYTA ESCOBAR** con **C.I. Nº 8327229 LP** y como titular derivado: **INSTITUTO DE INVESTIGACIONES INGENIERÍA EN PRODUCCIÓN EMPRESARIAL, UNIVERSIDAD PÚBLICA DE EL ALTO - UPEA** con **NIT Nº 122025022** representado legalmente por **CARLOS CONDORI TITIRICO.**

Quedando amparado su derecho conforme a Ley, salvando el mejor derecho que terceras personas pudieren demostrar.

Regístrese, Comuníquese y Archívese.

Abg. Carlos Alberto Soruco Arroyo
DIRECTOR DE DERECHO DE AUTOR
Y DERECHOS CONEXOS
SERVICIO NACIONAL DE PROPIEDAD INTELECTUAL

V°B° Henry Cahuaya Quino SENAPI

CASA/hcq.
c.c.Arch.

NB/ISO 9001 IBNORCA Signos Distintivos

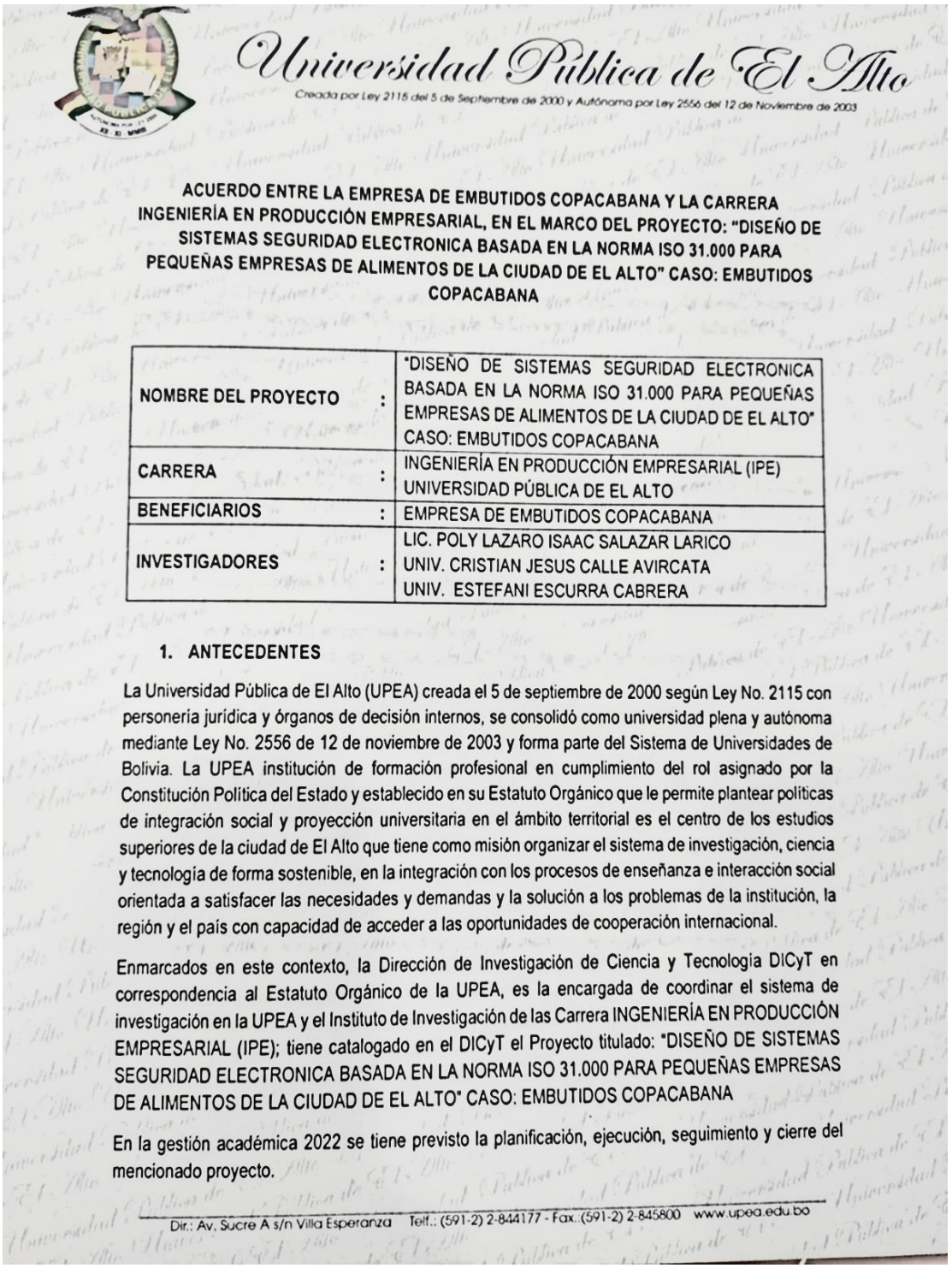
"2022 AÑO DE LA REVOLUCIÓN CULTURAL PARA LA DESPATRIARCALIZACIÓN: POR UNA VIDA LIBRE DE VIOLENCIA CONTRA LAS MUJERES"

HECHO EN BOLIVIA

Oficina Central - La Paz: Av. Montes, No 515, entre Esq. Uruguay y C. Batallón Illimani, Telfs.: 2115700 - 2119276 2119251 Fax: 2115700
Oficina - Santa Cruz: Av. Uruguay, Calle prolongación Quijarro, Nº 29, Edif. Bicentenario. Telfs.: 3121752 - 72042936
Oficina - Cochabamba: Calle Chuquisaca, Nº 649, Piso 2, entre Antezana y Lanza zona Central - Noreste. Telfs.: 4149403 - 72042957
Oficina - El Alto: Av. Juan Pablo II, Nº 2560 Edif. Multicentro El Ceibo Ltda. Piso 2, Of. 58, zona 16 de Julio. Telfs.: 2141001 - 72043029
Oficina - Chuquisaca: Calle Kilómetro 7, Nº 366 casi esq. Urriolagoitia, zona Parque Bolívar. Telf.: 72005873
Oficina - Tarija: Calle Ingavi, Nº 385 entre Santa Cruz y Méndez, zona La Pampa. Telf.: 72015286
Oficina - Oruro: Calle 6 de Octubre, Nº 5837, entre Ayacucho y Junín, Galería Central, Of. 14 (Ex Banco Fie). Telf.: 67201288
Oficina - Potosí: Av. Villazón entre calles Wencesalo Alba y San Alberto, Edif. AM. Salinas Nº 242, Primer Piso, Of. 17.

www.senapi.gob.bo

Anexo 2.- Acuerdo entre la empresa de Embutidos Copacabana y la carrera de Ingeniería en Producción Empresarial



Universidad Pública de El Alto

Creada por Ley 2115 del 5 de Septiembre de 2000 y Autónoma por Ley 2556 del 12 de Noviembre de 2003

ACUERDO ENTRE LA EMPRESA DE EMBUTIDOS COPACABANA Y LA CARRERA INGENIERÍA EN PRODUCCIÓN EMPRESARIAL, EN EL MARCO DEL PROYECTO: "DISEÑO DE SISTEMAS SEGURIDAD ELECTRONICA BASADA EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA

NOMBRE DEL PROYECTO	:	"DISEÑO DE SISTEMAS SEGURIDAD ELECTRONICA BASADA EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA
CARRERA	:	INGENIERÍA EN PRODUCCIÓN EMPRESARIAL (IPE) UNIVERSIDAD PÚBLICA DE EL ALTO
BENEFICIARIOS	:	EMPRESA DE EMBUTIDOS COPACABANA
INVESTIGADORES	:	LIC. POLY LAZARO ISAAC SALAZAR LARICO UNIV. CRISTIAN JESUS CALLE AVIRCATA UNIV. ESTEFANI ESCURRA CABRERA

1. ANTECEDENTES

La Universidad Pública de El Alto (UPEA) creada el 5 de septiembre de 2000 según Ley No. 2115 con personería jurídica y órganos de decisión internos, se consolidó como universidad plena y autónoma mediante Ley No. 2556 de 12 de noviembre de 2003 y forma parte del Sistema de Universidades de Bolivia. La UPEA institución de formación profesional en cumplimiento del rol asignado por la Constitución Política del Estado y establecido en su Estatuto Orgánico que le permite plantear políticas de integración social y proyección universitaria en el ámbito territorial es el centro de los estudios superiores de la ciudad de El Alto que tiene como misión organizar el sistema de investigación, ciencia y tecnología de forma sostenible, en la integración con los procesos de enseñanza e interacción social orientada a satisfacer las necesidades y demandas y la solución a los problemas de la institución, la región y el país con capacidad de acceder a las oportunidades de cooperación internacional.

Enmarcados en este contexto, la Dirección de Investigación de Ciencia y Tecnología DICyT en correspondencia al Estatuto Orgánico de la UPEA, es la encargada de coordinar el sistema de investigación en la UPEA y el Instituto de Investigación de las Carrera INGENIERÍA EN PRODUCCIÓN EMPRESARIAL (IPE); tiene catalogado en el DICyT el Proyecto titulado: "DISEÑO DE SISTEMAS SEGURIDAD ELECTRONICA BASADA EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA

En la gestión académica 2022 se tiene previsto la planificación, ejecución, seguimiento y cierre del mencionado proyecto.

Dir.: Av. Sucre A s/n Villa Esperanza Telf.: (591-2) 2-844177 - Fax.:(591-2) 2-845800 www.upea.edu.bo

Universidad Pública de El Alto

Creada por Ley 2115 del 5 de Septiembre de 2000 y Autónoma por Ley 2556 del 12 de Noviembre de 2003

2. DEL OBJETO

El presente acuerdo, tiene por objeto establecer una modalidad de implementación y ejecución del proyecto: "DISEÑO DE SISTEMAS SEGURIDAD ELECTRONICA BASADA EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA, entre la empresa de **Embutidos Copacabana** y la carrera **Ingeniería en Producción Empresarial (IPE)** dependiente de la **Universidad Pública de El Alto (UPEA)**.

3. ACUERDO DE PARTES

3.1. LA CARRERA INGENIERÍA EN PRODUCCIÓN EMPRESARIAL (IPE), POR INTERMEDIO DEL INSTITUTO DE INVESTIGACIÓN.

a) Se comprometen a realizar el trabajo de investigación titulado: **"DISEÑO DE SISTEMAS SEGURIDAD ELECTRONICA BASADA EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA,** trabajo que se realizará en cuatro módulos lecheros y las unidades de productores lecheros.
b) Realizar diferentes eventos relacionado con el diseño de sistemas de seguridad electrónica, en base a la identificación de vulnerabilidades y amenazas encontradas en la investigación, con profesionales entendidos en el tema.
c) Realizar seminarios de concientización sobre la seguridad electrónica dentro de una empresa.
d) Elaborar un diseño de los sistemas de seguridad electrónica para la empresa, como producto final del trabajo de investigación en base de un diseño presentado por el equipo de investigadores.
e) Realizar el plan trabajo sujeto a un cronograma que determine las actividades relacionadas para la investigación a realizarse entre la carrera de Ingeniería en Producción Empresarial y la empresa de embutidos Copacabana.

3.2. LA EMPRESA DE EMBUTIDOS "COPACABANA"

a) La empresa facilitará y autorizará el acceso a los ambientes de la empresa, a fin de facilitar el proceso de investigación para el diseño de los sistemas de seguridad electrónica.
b) La Empresa convocará a los encargados para la participación de los diferentes eventos programados en base a los requerimientos de la empresa.
c) La empresa de embutidos Copacabana, participará de manera activa con el personal de trabajo en las diferentes actividades programadas en base a un plan consensuado.
d) La empresa de embutidos Copacabana, prestará los ambientes para los cursos de capacitación, como también para el uso de los Docentes Investigadores en las diferentes actividades investigativas.

Dir.: Av. Sucre A s/n Villa Esperanza Telf.: (591-2) 2-844177 - Fax.:(591-2) 2-845800 www.upea.edu.bo

Universidad Pública de El Alto

Creada por Ley 2115 del 5 de Septiembre de 2000 y Autónoma por Ley 2556 del 12 de Noviembre de 2003

e) La empresa de embutidos Copacabana, publicará los resultados del diseño de los sistemas de seguridad electrónica a su personal, mediante capacitación y comunicados en la empresa.

Ambas partes declaran su intención de sistematizar las mejores experiencias resultantes del trabajo realizado, actualizando permanentemente la información generada con miras a futuras acciones conjuntas.

4. PLAZOS

El presente acuerdo, tendrá vigencia durante la gestión 2022, pudiendo ser ampliada, previa evaluación conjunta entre la empresa de embutidos Copacabana y la carrera de Ingeniería en Producción Empresarial (IPE) de la Universidad Pública de El Alto (UPEA).

5. ACEPTACIÓN DE LAS PARTES

Como muestra de conformidad del acuerdo entre partes, firman los representantes de las instituciones involucradas en el presente acuerdo.

FIRMAS DE CONFORMIDAD

Ingenieria en Producción Empresarial - IPE	M. Sc. Ing. Ronaldo René Nina Tinta DIRECTOR CARRERA INGENIERIA EN PRODUCCION EMPRESARIAL UNIVERSIDAD PUBLICA DE EL ALTO **M. Sc. Ing. Ronaldo René Nina Tinta** **C.I.: 6045127 LP**
Empresa de Embutidos Copacabana	Ing. Gonzalo Pizarro Ramos SUPERVISOR EMBUTIDOS COPACABANA **Gonzalo Pizarro Ramos** **C.I.: 9114910 LP**

Es dado, en fecha 14 de junio del 2022

Anexo 3.- Visita a los ambientes de elaboración de embutidos de la empresa

Anexo 4.- Presentación de informe a la empresa de Embutidos Copacabana

Universidad Pública de El Alto
Creada por Ley 3446 del 21 de septiembre de 2006 y ratificada por Ley 3838 del 13 de noviembre de 2008
VICERRECTORADO
DIRECCIÓN DE INVESTIGACIÓN CIENCIA Y TECNOLOGÍA

Área: Desarrollo Tecnológico Productivo
Carrera: Ingeniería en Producción Empresarial
Instituto de Investigación y Posgrado

INFORME IIPGIPE 1/2022

A : Ing. Gonzalo Pizarro Ramos
JEFE DE PRODUCCIÓN
EMPRESA DE EMBUTIDOS COPACABANA

DE : Lic. Poly Ubaldo Isaac Salazar Larico
DOCENTE INVESTIGADOR
INSTITUTO DE INVESTIGACIÓN Y POSGRADO
INGENIERIA EN PRODUCCIÓN EMPRESARIAL

REF. : INFORME DE RESULTADOS DEL ANALISIS DE RIESGO EMPRESA EMBUTIDOS COPACABANA.

FECHA : El Alto, octubre de 2022

De mi mayor consideración.

A tiempo de saludarle y desearle éxitos en sus funciones que desempeña, tengo a bien presentar el informe técnico de las actividades realizadas procurando dar cumplimiento a los objetivos propuestos en el proyecto "Diseño de sistemas de seguridad electrónica basado en la norma ISO 31.000 para pequeñas empresas de alimentos en la ciudad de El Alto. CASO: Embutidos Copacabana".

1 ANTECEDENTES.

En fecha 14/06/2022, mediante la firma de acuerdo realizado entre la empresa de embutidos Copacabana y la carrera de Ingeniería en Producción Empresarial de la Universidad Pública de El Alto en el marco del proyecto, "DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA, se tiene base legal para la modalidad y ejecución del proyecto.

2 OBJETIVO

Informar a la empresa de embutidos Copacabana los resultados conseguidos tras realizar la ejecución del proyecto DISEÑO DE SISTEMAS DE SEGURIDAD ELECTRÓNICA BASADO EN LA NORMA ISO 31.000 PARA PEQUEÑAS EMPRESAS DE ALIMENTOS DE LA CIUDAD DE EL ALTO" CASO: EMBUTIDOS COPACABANA.

Anexo 5.- Certificado de registro sanitario - SENASAG

ESTADO PLURINACIONAL DE BOLIVIA
SERVICIO NACIONAL DE SANIDAD AGROPECUARIA E INOCUIDAD ALIMENTARIA
SENASAG
LEY NACIONAL 2061

CERTIFICADO DE REGISTRO SANITARIO

No. 0583/2019

SE CERTIFICA

Que la Empresa : **PIZARRO SIÑANI ANTONIO**

Cumple con los Requisitos Sanitarios según Informe Técnico **UNIA-REG-INFTEC-04-85-2019**

Quedando registrada con el R.S. No.

04	02	03	02	0015

1.- Nivel de Mercado : **Nacional**

2.- Tipo de Empresa : **SEMI-INDUSTRIAL**

3.- Grupo de Productos : **De carne y derivados**

4.- Certificado Válido Hasta : **27 de febrero de 2024**

Este certificado debe exhibirse en forma permanente en la empresa.
Es cuanto certifica :
Que la Empresa ***PIZARRO SIÑANI ANTONIO***
Cumple con los Requisitos Sanitarios exigidos por el SENASAG

Ing. Edwin Rojas Maldonado
RESPONSABLE DEPARTAMENTAL
INOCUIDAD ALIMENTARIA
MDRyT SENASAG LA PAZ

Dra. Omar Hernán Ticona
DIRECTOR DEPARTAMENTAL
INOCUIDAD ALIMENTARIA
SENASAG - LA PAZ - MDRyT

SELLOS

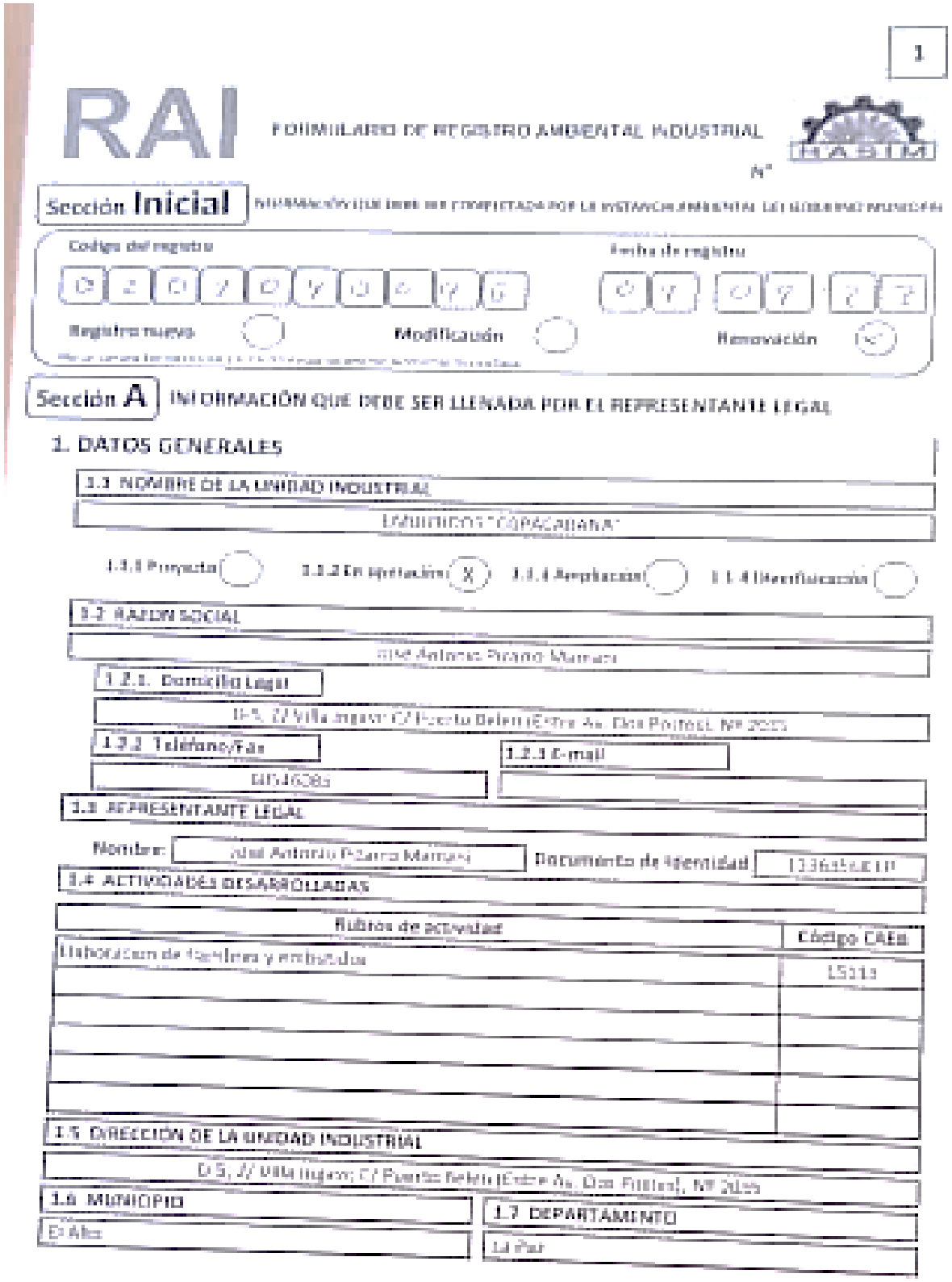
La Paz, 10 de mayo de 2019

NB/ISO 9001 IQNet IRNORCA

NOTA: Cualquier enmienda o corrección en el presente documento anulará su vigencia

Nº 105597

Anexo 6.- Certificado de registro ambiental industrial - RAI



1

RAI

FORMULARIO DE REGISTRO AMBIENTAL INDUSTRIAL

N°

Sección Inicial

Código del registro

Fecha de registro

Registro nuevo ( ) Modificación ( ) Renovación (X)

Sección A INFORMACIÓN QUE DEBE SER LLENADA POR EL REPRESENTANTE LEGAL

1. DATOS GENERALES

1.1 NOMBRE DE LA UNIDAD INDUSTRIAL

EMBUTIDOS "COPACABANA"

1.1.1 Proyecto ( ) 1.1.2 En Operación (X) 1.1.3 Ampliación ( ) 1.1.4 Reestructuración ( )

1.2 RAZON SOCIAL

José Antonio Pizarro Marnani

1.2.1. Domicilio Legal

D.S. 2/ Villa Ingavi C/ Puerto Belen (Entre Av. Dos Puentes) Nº 2555

1.2.2 Teléfono/Fax

1.2.3 E-mail

1.3 REPRESENTANTE LEGAL

Nombre: José Antonio Pizarro Marnani Documento de Identidad

1.4 ACTIVIDADES DESARROLLADAS

Rubros de actividad	Código CAEB
Elaboración de fiambres y embutidos	15111

1.5 DIRECCIÓN DE LA UNIDAD INDUSTRIAL

D.S. 2/ Villa Ingavi; C/ Puerto Belen (Entre Av. Dos Puentes), Nº 2555

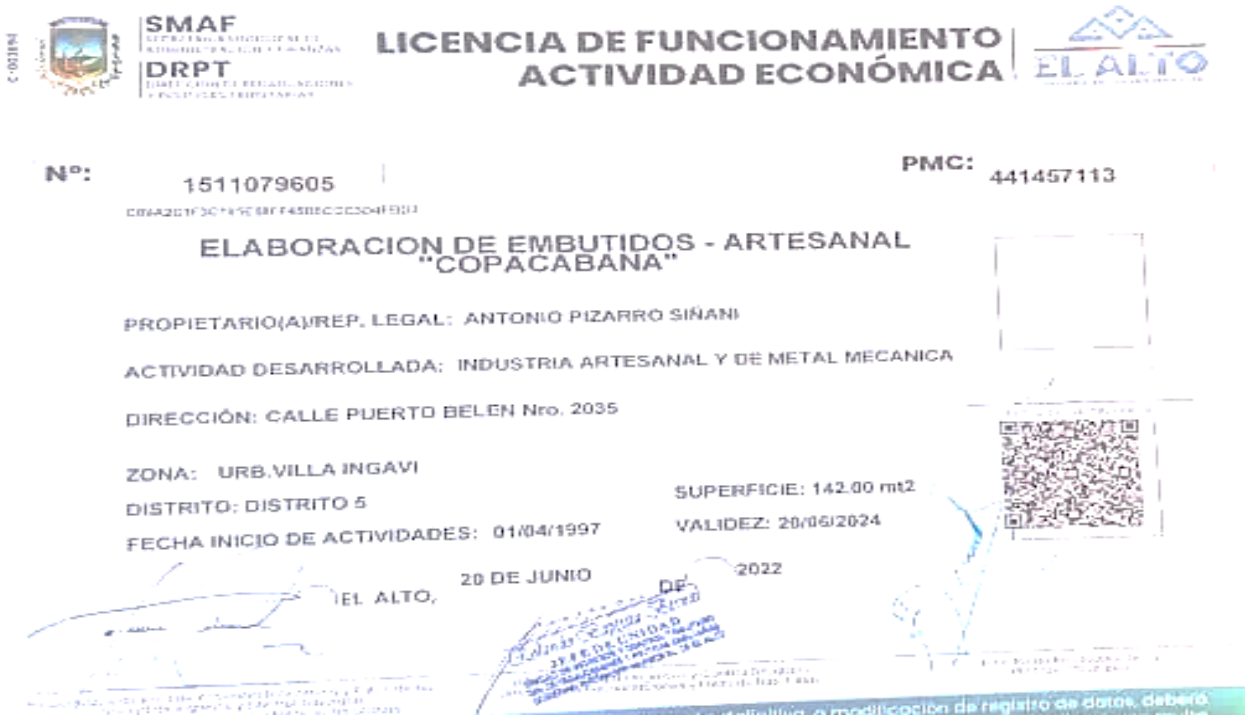
1.6 MUNICIPIO

El Alto

1.7 DEPARTAMENTO

La Paz

Anexo 7.- Licencia de funcionamiento de actividad económica



SMAF
DRPT

LICENCIA DE FUNCIONAMIENTO
ACTIVIDAD ECONÓMICA

EL ALTO

Nº: 1511079605

PMC: 441457113

ELABORACION DE EMBUTIDOS - ARTESANAL "COPACABANA"

PROPIETARIO(A)/REP. LEGAL: ANTONIO PIZARRO SIÑANI

ACTIVIDAD DESARROLLADA: INDUSTRIA ARTESANAL Y DE METAL MECANICA

DIRECCIÓN: CALLE PUERTO BELEN Nro. 2035

ZONA: URB.VILLA INGAVI

DISTRITO: DISTRITO 5

FECHA INICIO DE ACTIVIDADES: 01/04/1997

SUPERFICIE: 142.00 mt2

VALIDEZ: 20/06/2024

EL ALTO, 20 DE JUNIO DE 2022

Anexo 8.- Numero de identificación tributaria

NIT

RÉGIMEN TRIBUTARIO SIMPLIFICADO

CERTIFICADO DE INSCRIPCIÓN
PADRON NACIONAL DE CONTRIBUYENTES

NIT: 441457010

NOMBRE / RAZÓN SOCIAL: PIZARRO SIÑANI ANTONIO

DATOS GENERALES:

DOMICILIO FISCAL: CALLE PUERTO BELEN NRO 2035 ZONA VILLA INGAVI

DEPENDENCIA: EL ALTO

ALCALDÍA: El Alto

GRAN ACTIVIDAD ECONÓMICA: ARTESANO

CATEGORIA: 1

CAPITAL DECLARADO: 12 331 Bs

OBLIGACIONES:

FORM. 6123 - REGIMEN TRIBUTARIO SIMPLIFICADO - ALTA 29/10/2007 - BIMESTRAL

FECHA DE INSCRIPCIÓN AL PADRÓN:

FECHA DE EMISIÓN DEL CERTIFICADO:

IMPUESTOS NACIONALES

Anexo 9.- Visita técnica a la empresa “Embutidos Copacabana”


LAVESE LAS MANOS


SISTEMAS DE CONTROL DE ACCESOS
SISTEMAS DE INTRUSIÓN
DETECTORES
SENSORES
SISTEMAS DE CIRCUITO CERRADO DE TELEVISION
PULSADORES

Anexo 10.- Montaje de sistemas de seguridad electrónica